

Компьютерные сети

Цель: формирование системы фундаментальных знаний по анализу и проектированию:

- локальных сетей (для офисных и корпоративных информационных систем (ИС));
- глобальных ИС, в том числе систем Интернет, каналов и сетевого оборудования Интернет, Web - страниц, системы электронной почты и ведения электронной корреспонденции.

Задание: изучение архитектуры компьютерных сетей, программного обеспечения и методов их проектирования; получение практических навыков анализа, построения и использования, защиты от несанкционированного доступа к информации.

Тема: Основы сетевых технологий

1. Эволюция вычислительных сетей. Два корня сетей передачи данных

История любой отрасли науки или техники позволяет не только удовлетворить естественное любопытство, но и глубже понять сущность основных достижений в этой отрасли, а также выявить тенденции и правильно оценить перспективность тех или иных направлений развития.

Сети передачи данных, называемые также вычислительными или компьютерными сетями, являются результатом эволюции двух важнейших научно-технических отраслей современной цивилизации — компьютерных и телекоммуникационных технологий:

1. С одной стороны, сети передачи данных представляют собой частный случай распределенных вычислительных систем, в которых группа компьютеров согласованно выполняет набор взаимосвязанных задач, обмениваясь данными в автоматическом режиме.

2. С другой стороны, компьютерные сети могут рассматриваться как средство передачи информации на большие расстояния, для чего в них применяются методы кодирования и мультиплексирования данных, получившие развитие в различных телекоммуникационных системах.

Итак,

- **компьютерная сеть** — это набор компьютеров, связанных коммуникационной системой и снабженных соответствующим программным обеспечением, которое предоставляет пользователям сети доступ к ресурсам этого набора компьютеров;

- сеть могут образовывать компьютеры разных типов — небольшие микропроцессоры, рабочие станции, мини-компьютеры, персональные компьютеры или суперкомпьютеры;

- передачу сообщений между любой парой компьютеров сети обеспечивает коммуникационная система, которая может включать кабели, повторители, коммутаторы, маршрутизаторы и другие устройства;

- компьютерная сеть позволяет пользователю работать со своим

компьютером, как с автономным, и добавляет к этому возможность доступа к информационным и аппаратным ресурсам других компьютеров сети.

2. Появление первых вычислительных машин

Идея компьютера была предложена английским математиком Чарльзом Бэббиджем (Charles Babig) в середине девятнадцатого века. Однако его механическая "аналитическая машина" по-настоящему так и не заработала.

Подлинное рождение цифровых вычислительных машин произошло вскоре после окончания второй мировой войны. В середине 40-х были созданы первые ламповые вычислительные устройства. Для этого периода характерно следующее:

- компьютер представлял собой скорее предмет исследования, а не инструмент для решения каких-либо практических задач из других областей;
- одна и та же группа людей участвовала и в проектировании, и в эксплуатации, и в программировании вычислительной машины; программирование осуществлялось исключительно на машинном языке;
- не было никакого системного программного обеспечения, кроме библиотек математических и служебных подпрограмм;
- операционные системы еще не появились, все задачи организации вычислительного процесса решались вручную каждым программистом с пульта управления.

С середины 50-х годов начался следующий период в развитии вычислительной техники, связанный с появлением новой технической базы — полупроводниковых элементов. В этот период:

- выросло быстродействие процессоров, увеличились объемы оперативной и внешней памяти;
- компьютеры стали более надежными;
- появились первые алгоритмические языки, и, таким образом, к библиотекам математических и служебных подпрограмм добавился новый тип системного программного обеспечения - трансляторы;
- были разработаны первые системные управляющие программы — мониторы, которые автоматизировали всю последовательность действий оператора по организации вычислительного процесса.

3. Программные мониторы — первые операционные системы

Программные мониторы явились прообразом современных операционных систем, они стали первыми системными программами, предназначенными не для обработки данных, а для управления вычислительным процессом.

В ходе реализации мониторов был разработан формализованный язык управления заданиями, с помощью которого программист сообщал системе и оператору, какие действия и в какой последовательности он хотел бы выполнить на вычислительной машине. Типовой набор директив обычно включал признак начала отдельной работы, вызов транслятора, вызов загрузчика, признаки начала и конца исходных данных.

Оператор составлял пакет заданий, которые в дальнейшем без его участия последовательно запускались на выполнение монитором. Кроме того, монитор был способен самостоятельно обрабатывать наиболее распространенные аварийные ситуации, возникающие при работе пользовательских программ, такие как отсутствие исходных данных, переполнение регистров, деление на ноль, обращение к несуществующей области памяти и т. д.

4. Мультипрограммирование

Следующий важный период развития операционных систем относится к 1965—1975 годам. В это время в технической базе вычислительных машин произошел переход от отдельных полупроводниковых элементов типа транзисторов к интегральным микросхемам, что открыло путь к появлению следующего поколения компьютеров, представителем которого является, например, IBM/360.

В этот период были реализованы практически все основные механизмы, присущие современным ОС: мультипрограммирование, мультипроцессирование, поддержка многотерминального многопользовательского режима, виртуальная память, файловые системы, разграничение доступа и сетевая работа. В эти годы начинается расцвет системного программирования. Из направления прикладной математики, представляющего интерес для узкого круга специалистов, системное программирование превращается в отрасль индустрии, оказывающую непосредственное влияние на практическую деятельность миллионов людей.

Начались разработки в области мультипрограммирования.

Мультипрограммирование — способ организации вычислительного процесса, при котором в памяти компьютера находится одновременно несколько программ, попеременно выполняющихся на одном процессоре.

Мультипрограммирование было реализовано в двух вариантах:

- пакетная обработка;
- разделение времени.

Системы пакетной обработки предназначались для решения задач в основном вычислительного характера, не требующих быстрого получения результатов.

Главной целью и критерием эффективности систем пакетной обработки является максимальная пропускная способность, то есть решение максимального числа задач в единицу времени.

Для достижения этой цели в системах пакетной обработки используется следующая схема функционирования (рис. 1.2): в начале работы формируется пакет заданий, каждое задание содержит требование к системным ресурсам; из этого пакета заданий формируется мультипрограммный набор, то есть множество одновременно выполняемых задач. Для одновременного выполнения выбираются задачи[^] предъявляющие к ресурсам различные требования, так, чтобы обеспечивалась сбалансированная загрузка всех устройств вычислительной машины. Например, в мультипрограммном наборе желательно присутствие и вычислительных задач, и задач с интенсивным вводом-выводом. Таким образом, выбор нового задания из пакета заданий зависит от внутренней ситуации, складывающейся в системе, то есть выбирается "выгодное" задание.

Следовательно, в вычислительных системах, работающих под управлением пакетных ОС, невозможно гарантировать выполнение того или иного задания в течение определенного периода времени.

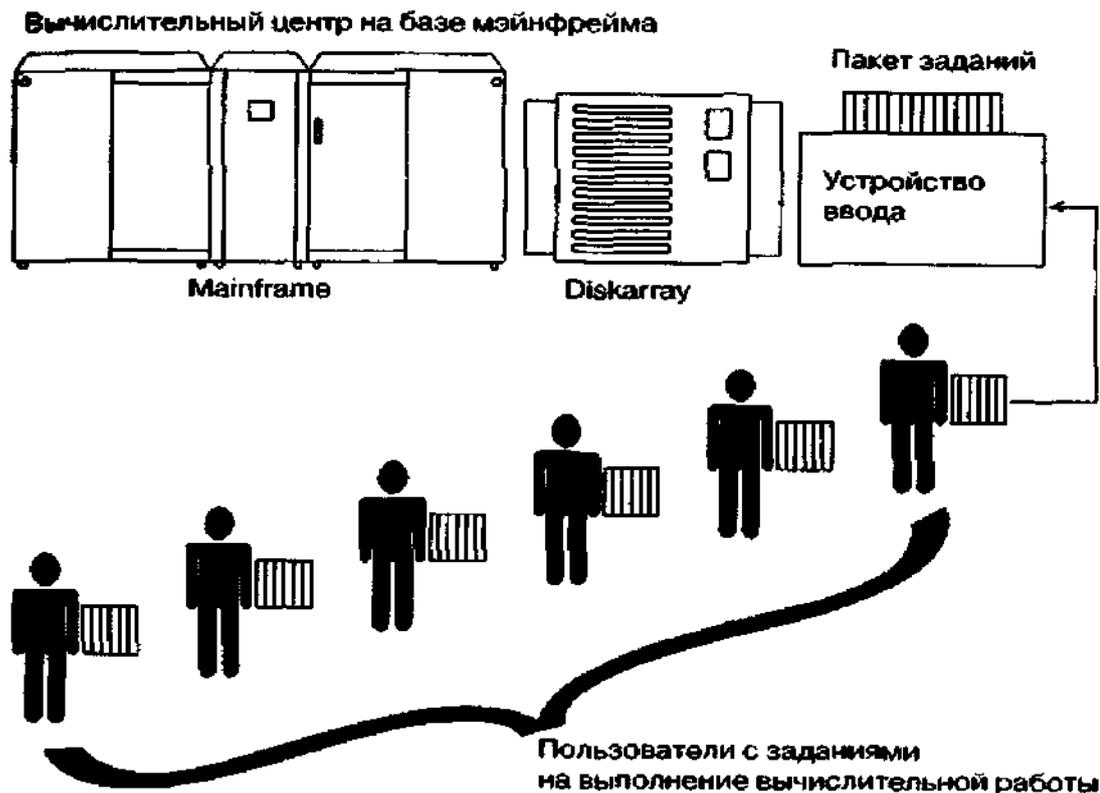


Рис. 1.2. Централизованный характер вычислений в системах пакетной обработки.

Взаимодействие пользователя с вычислительной машиной, на которой установлена система пакетной обработки, сводится к тому, что пользователь приносит задание, отдает его диспетчеру-оператору, а в конце дня после выполнения всего пакета заданий получает результат. Очевидно, что такой порядок повышает эффективность функционирования аппаратуры, но снижает эффективность работы пользователя.

В системах разделения времени пользователям (или одному пользователю) предоставляется возможность интерактивной работы сразу с несколькими приложениями. Для этого каждое приложение должно регулярно взаимодействовать с пользователем. Понятно, что в пакетных системах возможности диалога пользователя с приложением ограничены.

В системах разделения времени эта проблема решается за счет того, что ОС принудительно периодически приостанавливает приложения, не дожидаясь, когда они сами освободят процессор. Всем приложениям попеременно выделяется квант процессорного времени, таким образом, пользователи, запустившие программы на выполнение, получают возможность поддерживать с ними диалог.

Системы разделения времени призваны исправить основной недостаток систем пакетной обработки — изоляцию пользователя-программиста от

процесса выполнения задач. Каждому пользователю в этом случае предоставляется терминал, с которого он может вести диалог со своей программой. Так как в системах разделения времени каждой задаче выделяется только квант процессорного времени, ни одна задача не занимает процессор надолго, и время ответа оказывается приемлемым.

Ясно, что системы разделения времени обладают меньшей пропускной способностью, чем системы пакетной обработки, так как на выполнение принимается каждая запущенная пользователем задача, а не та, которая "выгодна" системе, производительность системы снижается из-за дополнительного расходования вычислительной мощности на более частое переключение процессора с задачи на задачу. **Это вполне соответствует тому, что [критерием эффективности систем разделения времени является не максимальная пропускная способность, а удобство и эффективность работы пользователя. Вместе с тем, мультипрограммное выполнение интерактивных приложений повышает и пропускную способность компьютера (пусть и не в такой степени, как пакетные системы). Аппаратура загружается лучше, поскольку пока одно приложение ждет сообщения пользователя, другие приложения могут обрабатываться процессором.**

5. Многотерминальные системы — прообраз сети

Терминалы, выйдя за пределы вычислительного центра, рассредоточились по всему предприятию. Многотерминальный режим использовался не только в системах разделения времени, но и в системах пакетной обработки. При этом не только оператор, но и все пользователи получали возможность формировать свои задания и управлять их выполнением со своего терминала. **Такие операционные системы получили название систем удаленного ввода заданий.**

Терминальные комплексы могли располагаться на большом расстоянии от процессорных стоек, соединяясь с ними с помощью различных глобальных связей — модемных соединений телефонных сетей или выделенных каналов. Для поддержки удаленной работы терминалов в операционных системах появились специальные программные модули, реализующие различные (в то время, как правило, нестандартные) протоколы связи. **Такие вычислительные системы с удаленными терминалами, сохраняя централизованный характер обработки данных, в какой-то степени являлись прообразом современных компьютерных сетей (рис. 1.3), а соответствующее системное программное обеспечение — прообразом сетевых операционных систем.**

Многотерминальные централизованные системы уже имели все внешние признаки локальных вычислительных сетей, однако, по существу ими не являлись, так как сохраняли сущность централизованной обработки данных автономно работающего компьютера.

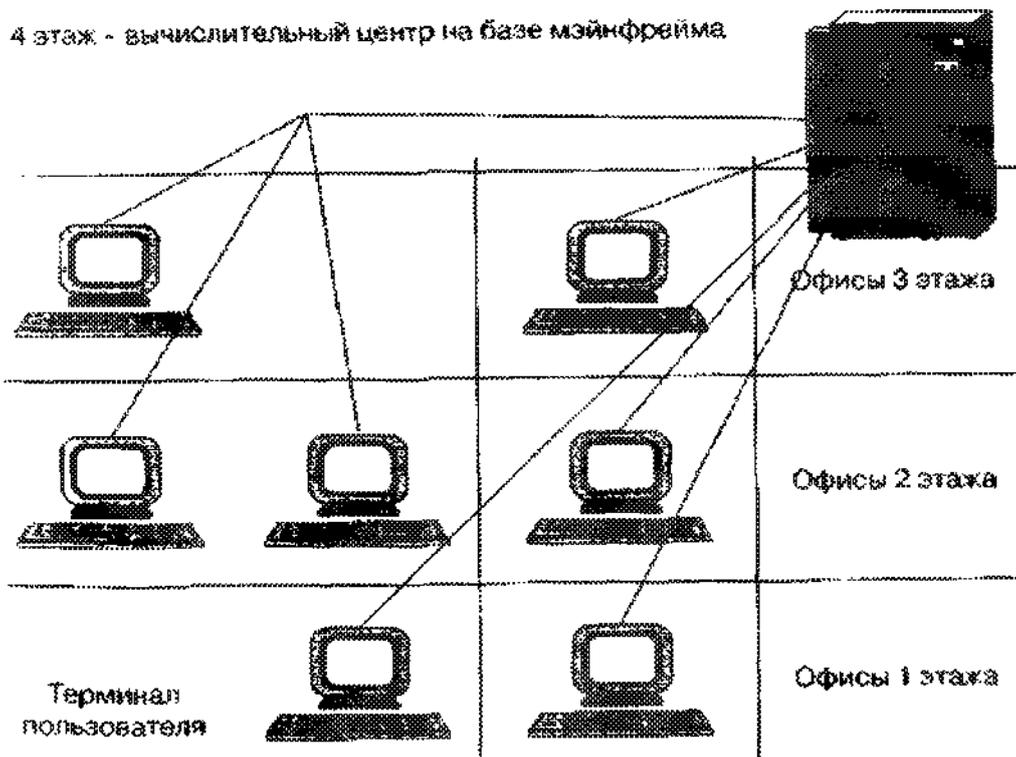


Рис. 1.3. Много терминальная система — прообраз вычислительной сети.

6. Компьютерные сети — частный случай распределенных вычислительных систем

Компьютерные сети, как уже было отмечено, являются продуктом эволюции телекоммуникационных и вычислительных систем. Компьютерные сети относятся к распределенным (или децентрализованным) вычислительным системам. Поскольку Основным признаком распределенной вычислительной системы является наличие нескольких центров обработки данных, то наряду с компьютерными сетями к распределенным системам относят также мультипроцессорные компьютеры и многомашинные вычислительные комплексы.

6.1 Мультипроцессорные компьютеры

В мультипроцессорных компьютерах имеется несколько процессоров, каждый из которых может относительно независимо от остальных выполнять свою программу. В мультипроцессоре существует общая для всех процессоров

операционная система, которая оперативно распределяет вычислительную нагрузку между процессорами, ν Взаимодействие между отдельными процессорами организуется наиболее простым способом — через общую оперативную память (рис. 1.5).

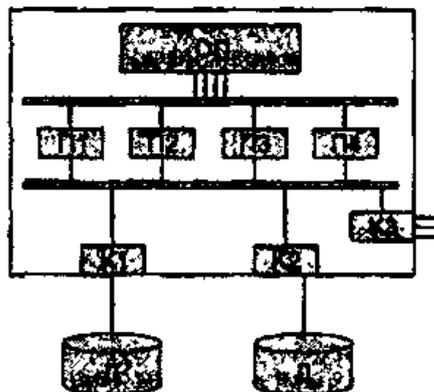


Рис. 1.5. Схема мультимикропроцессорной системы: ОП — оперативная память, П1–П4 — процессоры, К1–К3 — каналы ввода-вывода, Д — дисковые запоминающие устройства

Сам по себе процессорный блок не является законченным компьютером и поэтому не может выполнять программы без остальных блоков мультимикропроцессорного компьютера — памяти и периферийных устройств. Все периферийные устройства являются для всех процессоров мультимикропроцессорной системы общими. Мультимикропроцессору не свойственна территориальная распределенность — все его блоки располагаются в одном или нескольких близко расположенных конструктивах, как и у обычного компьютера.

Основное достоинство мультимикропроцессора — его высокая производительность, которая достигается за счет параллельной работы нескольких процессоров. Так как при наличии общей памяти взаимодействие процессоров происходит очень быстро, мультимикропроцессоры могут эффективно выполнять даже приложения с высокой степенью связи по данным.

Еще одним важным свойством мультимикропроцессорных систем является отказоустойчивость, то есть способность к продолжению работы при отказах некоторых элементов, например процессоров или блоков памяти. ν При этом производительность, естественно, снижается, но не до нуля, как в обычных системах, в которых отсутствует избыточность. Однако для того, чтобы мультимикропроцессор мог продолжать работу после отказа одного из процессоров, необходимо специальное программное обеспечение поддержки отказоустойчивости, которое может быть частью операционной системы или же представлять собой дополнительные служебные программы.

6.2 Кластеры

Кластер (многомашинная Система)

это вычислительный комплекс,

состоящий из нескольких компьютеров (каждый из которых работает под управлением собственной операционной системы), а также программные и аппаратные средства связи компьютеров, которые обеспечивают работу всех компьютеров комплекса как единого целого.

В отличие от мультимикропроцессора, в котором избыточность реализована на уровне процессорных блоков, кластер состоит из нескольких законченных, способных работать автономно, как правило, стандартных компьютеров, каждый из которых имеет обычную структуру, включающую один или несколько процессорных блоков, оперативную память и периферийные устройства (рис. 1.6). Однако благодаря специальному программному и аппаратному обеспечению межкомпьютерных связей для пользователя кластер выглядит как единый компьютер. При этом каждый компьютер (называемый также узлом кластера) может быть как микропроцессорным, так и мультимикропроцессорным на организацию кластера это влияния не оказывает.

Кластеры применяют для повышения надежности и производительности вычислительной системы. Надежность повышается за счет того, что при отказе одного из узлов кластера вычислительная нагрузка (или часть ее) переносится на другой узел. Для выполнения этой операции в кластере используется два типа связей между узлами: *межпроцессорные* связи и связи за счет *разделяемых дисков*.

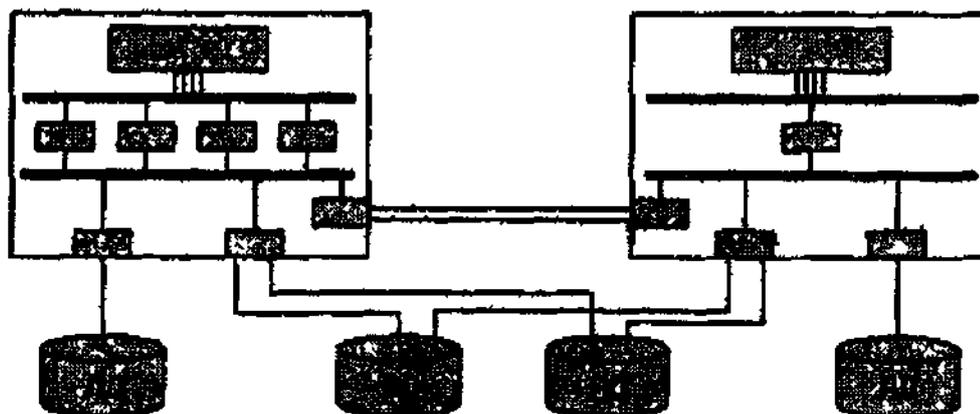


Рис. 1.6. Схема кластера

Межпроцессорные связи используются узлами для обмена служебной информацией. В частности, с помощью этих связей каждый узел кластера периодически проверяет состояние других узлов и выполняемых ими вычислительных задач. Если какой-либо узел или одна из его задач (входящая в набор защищаемых от отказов задач) изменили свое состояние на неработоспособное, то начинается процедура перемещения (реконфигурации) нагрузки на один из работоспособных узлов. В этой процедуре важную роль играют разделяемые диски. Защищаемая задача должна хранить свои данные на одном из таких дисков, чтобы новый узел смог продолжать их использовать после отказа основного. Так как надежность дисковых накопителей достаточно высока (ее можно повысить за счет дополнительных мер, например зеркалирования разделяемого диска), то существенно повышается и надежность кластера по

сравнению с отдельным компьютером. Время перевода нагрузки на другой узел кластера при отказе значительно больше, чем время перехода на другой процессор в мультипроцессоре, так как оно связано с активизацией новой копии программного процесса на другом узле. При этом также возможна потеря части данных, находившихся в оперативной памяти отказавшего узла, но для определенных типов вычислительной нагрузки, например систем управления базами данных или web-серверов, эти потери не сказываются на возможности продолжать вычисления.

Если кластер применяется для повышения производительности, то каждая задача, распараллеливается на несколько ветвей, которые выполняются одновременно на нескольких узлах кластера.

Синхронизация работы нескольких копий задачи или их ветвей, а также синхронизация вырабатываемых ими данных осуществляются как за счет межпроцессорных связей, так и за счет разделяемой дисковой памяти. Менее тесные и менее скоростные связи между узлами кластера по сравнению со связями процессоров в мультипроцессоре диктуют область применения кластеров — это задачи, достаточно независимые по данным.

Для организации межпроцессорных связей в кластерах часто используются специализированные технологии, приспособленные к решению специфических задач взаимодействия компьютеров в кластере. Однако в последнее время все чаще для этой цели применяются стандартные технологии локальных сетей, например Fast Ethernet и Gigabit Ethernet.

Совместный доступ к дискам также может осуществляться различными способами. Наиболее популярными вариантами является применение интерфейса SCSI и технологии Fibre Channel, тенденция перехода на стандартные технологии локальных сетей в этой области пока выражена не так отчетливо, как в области межпроцессорных связей, но она тоже имеется.

ЛОКАЛЬНЫЕ СЕТИ

1. Локальная вычислительная сеть

Локальная вычислительная сеть (ЛВС, *локальная сеть*; англ. *Local Area Network, LAN*) - компьютерная сеть, (**Компьютерная сеть (вычислительная сеть, сеть передачи данных)**) - система связи компьютеров или вычислительного оборудования (серверы, маршрутизаторы и другое оборудование). Для передачи данных могут быть использованы различные физические явления, как правило - различные виды электрических сигналов, световых сигналов или электромагнитного излучения.) покрывающая обычно относительно небольшую территорию или небольшую группу зданий (дом, офис, фирму, институт). Также существуют локальные сети, узлы которых разнесены географически на расстояния более 12 500 км (космические станции и орбитальные центры). Несмотря на такие расстояния, подобные сети всё равно относят к локальным.

Существует множество способов классификации сетей. Основным критерием классификации принято считать способ администрирования. То есть в зависимости от того, как организована сеть и как она управляется, её можно отнести к локальной, распределённой, городской или глобальной сети. Управляет сетью или её сегментом сетевой администратор. В случае сложных сетей их права и обязанности строго распределены, ведётся документация и журналирование действий команды администраторов.

Компьютеры могут соединяться между собой, используя различные среды доступа: медные проводники (витая пара), оптические проводники (оптические кабели) и через радиоканал (беспроводные технологии). Проводные, оптические связи устанавливаются через Ethernet, беспроводные - через Wi-Fi, Bluetooth, GPRS и прочие средства. Отдельная локальная вычислительная сеть может иметь связь с другими локальными сетями через шлюзы, а также быть частью глобальной вычислительной сети (например, Интернет) или иметь подключение к ней.

2. Витая пара. Оптическое волокно

Витая пара (англ. *twisted pair*) - вид кабеля связи, представляет собой одну или несколько пар изолированных проводников, скрученных между собой (с небольшим числом витков на единицу длины), покрытых пластиковой оболочкой.

Проводник - вещество, хорошо проводящее электрический ток; в таком веществе имеются свободные носители заряда, то есть заряженные частицы, которые могут свободно перемещаться внутри объёма вещества. Среди наиболее распространённых твёрдых проводников известны металлы, полуметаллы, углерод (в виде угля и графита). Пример проводящих жидкостей при нормальных условиях - ртуть, электролиты, при высоких температурах - расплавы металлов. Пример проводящих газов - ионизированный газ (плазма). Некоторые вещества, при нормальных условиях являющиеся изоляторами, при внешних воздействиях могут переходить в проводящее состояние, а именно проводимость полупроводников может сильно варьироваться при изменении температуры, освещённости, легировании и т. п.

Проводниками также называют части электрических цепей - соединительные провода и шины.

Свивание проводников производится с целью повышения степени связи между собой проводников одной пары (электромагнитные помехи одинаково влияют на оба провода пары) и последующего уменьшения электромагнитных помех от внешних источников, а также взаимных наводок при передаче дифференциальных сигналов. Для снижения связи отдельных пар кабеля (периодического сближения проводников различных пар) в кабелях UTP категории 5 и выше провода пары свиваются с различным шагом. Витая пара - один из компонентов современных структурированных кабельных систем. Используется в телекоммуникациях и в компьютерных сетях в качестве физической среды передачи сигнала во многих технологиях, таких как Ethernet,

Arcnet и Token ring. В настоящее время, благодаря своей дешевизне и лёгкости в монтаже, является самым распространённым решением для построения проводных (кабельных) локальных сетей.

Оптическое волокно - нить из оптически прозрачного материала (стекло, пластик), используемая для переноса света внутри себя посредством полного внутреннего отражения.

Волоконная оптика - раздел прикладной науки и машиностроения, описывающий такие волокна. Кабели на базе оптических волокон используются в волоконно-оптической связи, позволяющей передавать информацию на большие расстояния с более высокой скоростью передачи данных, чем в электронных средствах связи. В ряде случаев они также используются при создании датчиков.

Чаще всего локальные сети построены на технологиях [Ethernet](#) или [Wi-Fi](#). Следует отметить, что ранее использовались протоколы [Frame Relay](#), [Token ring](#), которые на сегодняшний день встречаются всё реже, их можно увидеть лишь в специализированных лабораториях, учебных заведениях и службах. Для построения простой локальной сети используются [маршрутизаторы](#), [коммутаторы](#), точки беспроводного доступа, беспроводные маршрутизаторы, [модемы](#) и сетевые адаптеры. Реже используются преобразователи (конвертеры) среды, усилители сигнала (повторители разного рода) и специальные антенны.

Иногда в локальной сети организуются *рабочие группы* - формальное объединение нескольких компьютеров в группу с единым названием.

Сетевой администратор — человек, ответственный за работу локальной сети или её части. В его обязанности входит обеспечение и контроль физической связи, настройка активного оборудования, настройка общего доступа и предопределённого круга программ, обеспечивающих стабильную работу сети.

Технологии локальных сетей реализуют, как правило, функции только двух нижних уровней модели OSI (базовая эталонная модель взаимодействия открытых систем) - физического и канального. Функциональности этих уровней

достаточно для доставки кадров в пределах стандартных топологий, которые поддерживают LAN: звезда (общая шина), кольцо и дерево. Однако из этого не следует, что компьютеры, связанные в локальную сеть, не поддерживают протоколы уровней, расположенных выше канального. Эти протоколы также устанавливаются и работают на узлах локальной сети, но выполняемые ими функции не относятся к технологии LAN

Маршрутизация в локальных сетях используется примитивная, если она вообще необходима. Чаще всего это статическая либо динамическая маршрутизация (основанная на протоколе [RIP](#)).

3. Сетевая модель OSI

Сетевая модель OSI ([англ. open systems interconnection basic reference model](#) - базовая эталонная модель взаимодействия открытых систем, сокр. ЭМВОС; 1978 г) - сетевая_модель стека сетевых протоколов OSI/ISO (ГОСТ Р ИСО/МЭК 7498-1-99).

Стек ([англ. stack](#) - стопка) - структура данных, представляющая собой список элементов, организованных по принципу LIFO ([англ. last in - first out](#), «последним пришёл - первым вышел»).

В связи с затянувшейся разработкой протоколов OSI, в настоящее время основным используемым стеком протоколов является **TCP/IP**, он был разработан ещё до принятия модели OSI и вне связи с ней.

В литературе наиболее часто принято начинать описание уровней модели OSI с 7-го уровня, называемого прикладным, и заканчивать 1-м уровнем – физическим.

Любой протокол модели OSI должен взаимодействовать либо с протоколами своего уровня, либо с протоколами на единицу выше и/или ниже своего уровня. Взаимодействия с протоколами своего уровня называются **горизонтальными**, а с уровнями на единицу выше или ниже - **вертикальными**. Любой протокол модели OSI может выполнять только функции своего уровня и не может выполнять функций другого уровня, что не выполняется в протоколах

альтернативных моделей.

Уровни модели OSI

Модель OSI		
Тип данных	Уровень (layer)	Функции
Данные	7. Прикладной (application)	Доступ к сетевым службам
Поток	6. Представления (presentation)	Представление и шифрование данных
Сеансы	5. Сеансовый (session)	Управление сеансом связи
Сегменты / Датаграммы	4. Транспортный (transport)	Прямая связь между конечными пунктами и надежность
Пакеты	3. Сетевой (network)	Определение маршрута и логическая адресация
Кадры	2. Канальный (data link)	Физическая адресация
Биты	1. Физический (physical)	Работа со средой передачи, сигналами и двоичными данными

Каждому уровню с некоторой долей условности соответствует свой **операнд** - логически неделимый элемент данных, которым на отдельном уровне можно оперировать в рамках модели и используемых протоколов: на физическом уровне мельчайшая единица - бит, на канальном уровне информация объединена в кадры, на сетевом - в пакеты (датаграммы), на транспортном - в сегменты. Любой фрагмент данных, логически объединённых для передачи - кадр, пакет, датаграмма - считается сообщением. Именно сообщения в общем виде являются операндами сеансового, представительского и прикладного уровней.

К базовым сетевым технологиям относятся физический и канальный уровни.

Прикладной уровень

Прикладной уровень (уровень приложений; англ. *application layer*) - верхний уровень модели, обеспечивающий взаимодействие пользовательских приложений с сетью:

1. позволяет приложениям использовать сетевые службы;
2. удалённый доступ к файлам и базам данных,
3. пересылка электронной почты;
4. отвечает за передачу служебной информации;
5. предоставляет приложениям информацию об ошибках;
6. формирует запросы к уровню представления.

Протоколы прикладного уровня: RDP (Remote Desktop Protocol), HTTP (HyperText Transfer Protocol), SMTP (Simple Mail Transfer Protocol), SNMP (Simple Network Management Protocol), POP3 (Post Office Protocol Version 3), FTP (File Transfer Protocol), XMPP (Extensible Messaging and Presence Protocol), OSCAR (Open System for CommunicAtion in Realtime), Modbus, SIP (Session Initiation Protocol), TELNET и другие.

Уровень представления

Уровень представления (англ. *presentation layer*, ошибочно называемый представительским уровнем) обеспечивает преобразование протоколов и шифрование/дешифрование данных. Запросы приложений, полученные с прикладного уровня, на уровне представления преобразуются в формат для передачи по сети, а полученные из сети данные преобразуются в формат приложений. На этом уровне может осуществляться сжатие/распаковка или кодирование/декодирование данных, а также перенаправление запросов другому сетевому ресурсу, если они не могут быть обработаны локально.

Уровень представлений обычно представляет собой промежуточный протокол для преобразования информации из соседних уровней. Это позволяет

осуществлять обмен между приложениями на разнородных компьютерных системах прозрачным для приложений образом. Уровень представлений обеспечивает форматирование и преобразование кода. Форматирование кода используется для того, чтобы гарантировать приложению поступление информации для обработки, которая имела бы для него смысл. При необходимости этот уровень может выполнять перевод из одного формата данных в другой.

Уровень представлений имеет дело не только с форматами и представлением данных, он также занимается структурами данных, которые используются программами. Таким образом, уровень 6 обеспечивает организацию данных при их пересылке.

Протоколы уровня представления: AFP - Apple Filing Protocol, ICA - Independent Computing Architecture, LPP - Lightweight Presentation Protocol, NCP - NetWare Core Protocol, NDR - Network Data Representation, XDR - eXternal Data Representation, X.25 PAD - Packet Assembler/Disassembler Protocol.

Сеансовый уровень

Сеансовый уровень (англ. session layer) модели обеспечивает поддержание сеанса связи, позволяя приложениям взаимодействовать между собой длительное время. Уровень управляет созданием/завершением сеанса, обменом информацией, синхронизацией задач, определением права на передачу данных и поддержанием сеанса в периоды неактивности приложений.

Протоколы сеансового уровня: ADSP (AppleTalk Data Stream Protocol), ASP (AppleTalk Session Protocol), H.245 (Call Control Protocol for Multimedia Communication), ISO-SP (OSI Session Layer Protocol (X.225, ISO 8327)), iSNS (Internet Storage Name Service), L2F (Layer 2 Forwarding Protocol), L2TP (Layer 2 Tunneling Protocol), NetBIOS (Network Basic Input Output System), PAP (Password Authentication Protocol), PPTP (Point-to-Point Tunneling Protocol), RPC (Remote Procedure Call Protocol), RTCP (Real-time Transport Control Protocol), SMPP (Short

Message Peer-to-Peer), SCP (Session Control Protocol), ZIP (Zone Information Protocol), SDP (Sockets Direct Protocol).

Транспортный уровень

Транспортный уровень (англ. *transport layer*) модели предназначен для обеспечения надёжной передачи данных от отправителя к получателю. При этом уровень надёжности может варьироваться в широких пределах. Существует множество классов протоколов транспортного уровня, начиная от протоколов, предоставляющих только основные транспортные функции (например, функции передачи данных без подтверждения приема), и заканчивая протоколами, которые гарантируют доставку в пункт назначения нескольких пакетов данных в надлежащей последовательности, мультиплексируют несколько потоков данных, обеспечивают механизм управления потоками данных и гарантируют достоверность принятых данных. Например, UDP ограничивается контролем целостности данных в рамках одной датаграммы и не исключает возможности потери пакета целиком или дублирования пакетов, нарушения порядка получения пакетов данных; TCP обеспечивает надёжную непрерывную передачу данных, исключаящую потерю данных или нарушение порядка их поступления или дублирования, может перераспределять данные, разбивая большие порции данных на фрагменты и, наоборот, склеивая фрагменты в один пакет.

Протоколы транспортного уровня: ATP (AppleTalk Transaction Protocol), CUDP (Cyclic UDP), DCCP (Datagram Congestion Control Protocol), FCP (Fiber Channel Protocol), IL (IL Protocol), NBF (NetBIOS Frames protocol), NCP (NetWare Core Protocol), RTP (Real-time Transport Protocol), SCTP (Stream Control Transmission Protocol), SPX (Sequenced Packet Exchange), SST (Structured Stream Transport), TCP (Transmission Control Protocol), UDP (User Datagram Protocol).

Сетевой уровень

Сетевой уровень (англ. *network layer*) модели предназначен для определения пути передачи данных. Отвечает за трансляцию логических адресов и имён в физические, определение кратчайших маршрутов, коммутацию и маршрутизацию, отслеживание неполадок и «заторов» в сети.

Протоколы сетевого уровня маршрутизируют данные от источника к получателю. Работающие на этом уровне устройства (маршрутизаторы) условно называют устройствами третьего уровня (по номеру уровня в модели OSI).

Протоколы сетевого уровня: IP/IPv4/IPv6 (Internet Protocol), IPX (Internetwork Packet Exchange, протокол межсетевого обмена), X.25 (частично этот протокол реализован на уровне 2), CLNP (сетевой протокол без организации соединений), IPsec (Internet Protocol Security). Протоколы маршрутизации - RIP (Routing Information Protocol), OSPF (Open Shortest Path First).

Канальный уровень

Канальный уровень (англ. *data link layer*) предназначен для обеспечения взаимодействия сетей по физическому уровню и контролем над ошибками, которые могут возникнуть. Полученные с физического уровня данные, представленные в битах, он упаковывает в кадры, проверяет их на целостность и, если нужно, исправляет ошибки (формирует повторный запрос поврежденного кадра) и отправляет на сетевой уровень. Канальный уровень может взаимодействовать с одним или несколькими физическими уровнями, контролируя и управляя этим взаимодействием.

Спецификация IEEE 802 разделяет этот уровень на два подуровня: MAC (англ. *media access control*) регулирует доступ к разделяемой физической среде, LLC (англ. *logical link control*) обеспечивает обслуживание сетевого уровня.

На этом уровне работают коммутаторы, мосты и другие устройства. Эти устройства используют адресацию второго уровня (по номеру уровня в модели

OSI).

Протоколы канального уровня- ARCnet, ATM, Controller Area Network (CAN), Econet, Ethernet, Ethernet Automatic Protection Switching (EAPS), Fiber Distributed Data Interface (FDDI), Frame Relay, High-Level Data Link Control (HDLC), IEEE 802.2 (provides LLC functions to IEEE 802 MAC layers), Link Access Procedures, D channel (LAPD), IEEE 802.11 wireless LAN, LocalTalk, Multiprotocol Label Switching (MPLS), Point-to-Point Protocol (PPP), Point-to-Point Protocol over Ethernet (PPPoE), Serial Line Internet Protocol (SLIP, устарел), StarLan, Token ring, Unidirectional Link Detection (UDLD), x.25.

В программировании этот уровень представляет драйвер (Драйвер (англ. *driver*, мн. ч. *драйверы*) - компьютерная программа, с помощью которой другие программы (операционная система) получают доступ к аппаратному обеспечению некоторого устройства) сетевой платы, в операционных системах имеется программный интерфейс взаимодействия канального и сетевого уровней между собой. Это не новый уровень, а просто реализация модели для конкретной ОС. Примеры таких интерфейсов: ODI, NDIS, UDI.

Физический уровень

Физический уровень (англ. *physical layer*) - нижний уровень модели, который определяет метод передачи данных, представленных в двоичном виде, от одного устройства (компьютера) к другому. Составлением таких методов занимаются разные организации, в том числе: Институт инженеров по электротехнике и электронике, Альянс электронной промышленности, Европейский институт телекоммуникационных стандартов и другие.

Эти методы осуществляют передачу электрических или оптических сигналов в кабель или в радиоэфир и, соответственно, их приём и преобразование в биты данных в соответствии с методами кодирования цифровых сигналов.

На этом уровне также работают концентраторы, повторители сигнала и медиаконвертеры.

Функции физического уровня реализуются на всех устройствах,

подключенных к сети. Со стороны компьютера функции физического уровня выполняются сетевым адаптером или последовательным портом. К физическому уровню относятся физические, электрические и механические интерфейсы между двумя системами. Физический уровень определяет такие виды сред передачи данных как оптоволокно, витая пара, коаксиальный кабель, спутниковый канал передач данных и т. п. Стандартными типами сетевых интерфейсов, относящимися к физическому уровню, являются: V.35, RS-232, RS-485, RJ-11, RJ-45, разъемы AUI и BNC.

Протоколы физического уровня: IEEE 802.15 (Bluetooth), IRDA, EIA RS-232, EIA-422, EIA-423, RS-449, RS-485, DSL, ISDN, SONET/SDH, 802.11 Wi-Fi, Etherloop, GSM Um radio interface, ITU и ITU-T, TransferJet, ARINC 818, G.hn/G.9960.

4. Маршрутизаторы

Маршрутиза́тор (от англ. router) - специализированный сетевой компьютер, имеющий как минимум один сетевой интерфейс и пересылающий пакеты данных между различными сегментами сети, связывающий разнородные сети различных архитектур, принимающий решения о пересылке на основании информации о топологии сети (Сетевая тополóгия (от греч. τόπος, - место) - способ описания конфигурации сети, схема расположения и соединения сетевых устройств) и определённых правил, заданных администратором.

Маршрутизатор работает на более высоком «сетевом» уровне 3 сетевой модели OSI, нежели коммутатор (или сетевой мост) и концентратор (хаб), которые работают соответственно на уровне 2 и уровне 1 модели OSI.

Принцип работы

Обычно маршрутизатор использует адрес получателя, указанный в пакетных данных, и определяет по таблице маршрутизации путь, по которому следует передать данные. Если в таблице маршрутизации для адреса нет описанного маршрута, пакет отбрасывается.

Существуют и другие способы определения маршрута пересылки пакетов, когда, например, используется адрес отправителя, используемые протоколы верхних уровней и другая информация, содержащаяся в заголовках пакетов сетевого уровня. Нередко маршрутизаторы могут осуществлять трансляцию адресов отправителя и получателя, фильтрацию транзитного потока данных на основе определённых правил с целью ограничения доступа, шифрование/расшифрование передаваемых данных и т. д.

Таблица маршрутизации

Таблица маршрутизации содержит информацию, на основе которой маршрутизатор принимает решение о дальнейшей пересылке пакетов. Таблица состоит из некоторого числа записей - маршрутов, в каждой из которых содержится адрес сети получателя, адрес следующего узла, которому следует передавать пакеты, административное расстояние - степень доверия к источнику маршрута и некоторый вес записи - метрика. Метрики записей в таблице играют роль в вычислении кратчайших маршрутов к различным получателям. В зависимости от модели маршрутизатора и используемых протоколов маршрутизации, в таблице может содержаться некоторая дополнительная служебная информация.

Административное расстояние - это функция, используемая маршрутизаторами для выбора оптимального маршрута при наличии двух и более различных маршрутов до одной цели по различным протоколам маршрутизации. Административное расстояние определяет надёжность протокола маршрутизации. Каждому протоколу маршрутизации назначается приоритет надёжности (достоверности), от максимального до минимального, указанный с помощью значения административного расстояния.

Протокол маршрутизации - сетевой протокол, используемый маршрутизаторами для определения возможных маршрутов следования данных в составной компьютерной сети. Применение протокола маршрутизации позволяет избежать ручного ввода всех допустимых маршрутов, что, в свою очередь, снижает количество ошибок, обеспечивает согласованность действий всех

маршрутизаторов в сети и облегчает труд администраторов.

Сетевой протокол - набор правил и действий (очередности действий), позволяющий осуществлять соединение и обмен данными между двумя и более включёнными в сеть устройствами.

Протоколы **маршрутизации** делятся на два вида, зависящие от типов алгоритмов, на которых они основаны:

- Дистанционно-векторные протоколы, основаны на Distance Vector Algorithm (DVA);
- Протоколы состояния каналов связи, основаны на Link State Algorithm (LSA).

Так же протоколы маршрутизации делятся на два вида в зависимости от сферы применения:

- Междоменной маршрутизации;
- Внутримоменной маршрутизации.

Домен (фр. *domaine*) — область; единица структуры. Доменное имя — символьное имя, помогающее находить адреса интернет-серверов

Таблица маршрутизации может составляться двумя способами:

- **статическая маршрутизация** - когда записи в таблице вводятся и изменяются вручную. Такой способ требует вмешательства администратора каждый раз, когда происходят изменения в топологии сети. С другой стороны, он является наиболее стабильным и требующим минимума аппаратных ресурсов маршрутизатора для обслуживания таблицы.

- **динамическая маршрутизация** - когда записи в таблице обновляются автоматически при помощи одного или нескольких протоколов маршрутизации - RIP, OSPF, IGRP, EIGRP, IS-IS, BGP, и др. Кроме того, маршрутизатор строит таблицу оптимальных путей к сетям назначения на основе различных критериев - количества промежуточных узлов, пропускной способности каналов, задержки передачи данных и т. п. Критерии вычисления оптимальных маршрутов чаще всего зависят от протокола маршрутизации, а также задаются конфигурацией маршрутизатора. Такой способ построения таблицы позволяет автоматически держать таблицу маршрутизации в актуальном

состоянии и вычислять оптимальные маршруты на основе текущей топологии сети. Однако динамическая маршрутизация оказывает дополнительную нагрузку на устройства, а высокая нестабильность сети может приводить к ситуациям, когда маршрутизаторы не успевают синхронизировать свои таблицы, что приводит к противоречивым сведениям о топологии сети в различных её частях и потере передаваемых данных.

Зачастую для построения таблиц маршрутизации используют теорию графов.

Применение

Маршрутизаторы помогают уменьшить загрузку сети, благодаря её разделению на домены коллизий (Другими словами - это сегмент сети, имеющий общий канальный уровень (Data Link layer) модели OSI, в котором передать фрейм может только один абонент одновременно. Задержка распространения фреймов между станциями, либо одновременное начало передачи вызывает возникновение коллизий, которые требуют специальной обработки и снижают производительность сети) или широковещательные домены, а также благодаря фильтрации пакетов. В основном их применяют для объединения сетей разных типов, зачастую несовместимых по архитектуре и протоколам, например для объединения локальных сетей Ethernet и WAN-соединений, использующих протоколы xDSL, PPP, ATM, Frame relay и т. д. Нередко маршрутизатор используется для обеспечения доступа из локальной сети в глобальную сеть Интернет, осуществляя функции трансляции адресов и межсетевое экран.

В качестве маршрутизатора может выступать как специализированное (аппаратное) устройство, так и обычный компьютер, выполняющий функции маршрутизатора. Существует несколько пакетов программного обеспечения (на основе ядра Linux, на основе операционных систем BSD) с помощью которого можно превратить ПК в высокопроизводительный и многофункциональный маршрутизатор, например, Quagga, IPFW или простой в применении PF.

Устройства для дома и малого офиса

В бытовом секторе обычно используются малопортовые маршрутизаторы/роутеры, обеспечивающие подключение домашней сети компьютеров к каналу связи провайдера интернета. Как правило, при этом роутер обеспечивает IP-адресацию устройств локальной сети по протоколу DHCP, а сам получает IP-адрес от внешнего провайдера. Обычно современный роутер имеет ряд вспомогательных функций и встроенных возможностей: точка доступа Wi-Fi для подключения мобильных устройств, файервол для защиты сети от внешних атак, резервирование интернета от нескольких провайдеров, веб-интерфейс для упрощения настройки устройства, USB-порт для подключения принтера или дискового хранилища и другие. Бытовые маршрутизаторы имеют различную сетевую пропускную способность, простые дешёвые модели могут ограничивать скорость подключения интернет на высокоскоростных тарифах.

5. Протокол передачи данных. Интерфейс

Протокол передачи данных - набор соглашений интерфейса *логического уровня*, которые определяют обмен данными между различными программами. Эти соглашения задают единообразный способ передачи сообщений и обработки ошибок при взаимодействии программного обеспечения разнесённой в пространстве аппаратуры, соединённой тем или иным интерфейсом.

Стандартизированный протокол передачи данных также позволяет разрабатывать интерфейсы (уже на *физическом уровне*), не привязанные к конкретной аппаратной платформе и производителю (например, USB, Bluetooth).

Интерфейс (англ. interface - *сопряжение, поверхность раздела, перегородка*) - совокупность возможностей, способов и методов взаимодействия двух систем (любых, а не обязательно являющиеся вычислительными или информационными), устройств или программ для обмена информацией между ними, определённая их характеристиками, характеристиками соединения, сигналов обмена и т. п. В случае, если одна из взаимодействующих систем - человек, чаще говорят лишь о второй системе, то есть об интерфейсе той системы, с которой человек взаимодействует.

Примеры:

- руль, педали газа и тормоза, ручка КПП - интерфейс (управления) автомобиля или же интерфейс системы «водитель - автомобиль»;
- элементы электронного аппарата (телевизора, автомагнитолы, часов и т. п.) - дисплей, набор кнопок и переключателей для настройки, плюс правила управления ими - интерфейс системы «человек - аппарат»;
- клавиатура, мышь и пр. устройства ввода - элементы сопряжения в системе пользовательского интерфейса (в свою очередь, и сами клавиатура и мышь имеют свои интерфейсы сопряжения с компьютером, аппаратные и программные).

Наиболее часто этот термин применяется в **информатике**, где это - совокупность унифицированных технических и программных средств и правил

(описаний, соглашений, протоколов), обеспечивающих взаимодействие устройств и/или программ в вычислительной системе или сопряжение между системами.

Интерфейсы являются основой взаимодействия всех современных информационных систем. Если интерфейс какого-либо объекта (персонального компьютера, программы, функции) не изменяется (стабилен, стандартизирован), это даёт возможность модифицировать сам объект, не перестраивая принципы его взаимодействия с другими объектами (так, например, научившись работать с одной программой под Windows, пользователь с лёгкостью освоит и другие — потому, что они имеют однотипные элементы интерфейса).

В вычислительной системе взаимодействие может осуществляться на **пользовательском, программном и аппаратном уровнях**.

Соответственно, согласно этому, **интерфейсы могут существовать как:**

1 Способ взаимодействия физических устройств

Физический (аппаратный) интерфейс — способ взаимодействия физических устройств. Чаще всего речь идёт о компьютерных портах.

- Сетевой интерфейс
- Сетевой шлюз — устройство, соединяющее локальную сеть с более крупной, например, Интернетом
- Шина (компьютер)

2 Способ взаимодействия виртуальных устройств

Для виртуальных (программных) устройств существуют следующие интерфейсы (Программный интерфейс):

- Интерфейс функции
- Интерфейс программирования приложений (API) — набор стандартных библиотечных методов, которые программист может использовать для доступа к функциональности другой программы.
- Удалённый вызов процедур
- СОМ-интерфейс
- Интерфейс объектно-ориентированного программирования

3 Способ взаимодействия человек-машина

Совокупность средств, при помощи которых пользователь взаимодействует с различными программами и устройствами (Интерфейс пользователя):

- Интерфейс командной строки: инструкции компьютеру даются путём ввода с клавиатуры текстовых строк (команд).
 - Графический интерфейс пользователя: программные функции представляются графическими элементами экрана.
 - Диалоговый интерфейс: например, Поиск
 - Жестовый интерфейс: сенсорный экран, руль, джойстик и т. д.
 - Естественно-языковой интерфейс, применяемый в интеллектуальных системах, пользователь «разговаривает» с программой на родном ему языке.
 - Нейрокомпьютерный интерфейс: отвечает за обмен между нейронами и электронным устройством при помощи специальных имплантированных электродов.
- и др.

6. Беспроводная точка доступа

Беспроводная точка доступа (англ. *Wireless Access Point*, WAP) - это беспроводная базовая станция (**Базовая станция** в радиосвязи вообще - системный комплекс приёмопередающей аппаратуры, осуществляющей централизованное обслуживание группы оконечных абонентских устройств), предназначенная для обеспечения беспроводного доступа к уже существующей сети (беспроводной или проводной) или создания новой беспроводной сети.

Введение

Объединение компьютеров в проводную сеть обычно требует прокладки множества кабелей через стены и потолки. Также проводные сети накладывают определённые ограничения на расположение устройств в пространстве. Этих недостатков лишены беспроводные сети: можно добавлять компьютеры и прочие беспроводные устройства с минимальными физическими, временными и материальными затратами. Для передачи информации беспроводные точки

доступа используют радиоволны из спектра частот, определённых стандартом IEEE 802.11.

Использование

Чаще всего беспроводные точки доступа используются для предоставления доступа мобильным устройствам (ноутбуки, принтеры и т. д.) к стационарной локальной сети.

Также беспроводные точки доступа часто используются для создания так называемых «горячих точек» - областей, в пределах которых клиенту предоставляется, как правило, бесплатный доступ к сети Интернет. Обычно такие точки находятся в библиотеках, аэропортах, уличных кафе крупных городов.

В последнее время наблюдается повышение интереса к беспроводным точкам доступа при создании домашних сетей. Для создания такой сети в пределах одной квартиры достаточно одной точки доступа. Возможно, этого будет достаточно для включения в сеть и соседей прилегающих квартир. Для включения в сеть квартиры через одну, определенно, потребуются ещё одна точка доступа, которая будет служить ретранслятором сигнала, ослабевшего вследствие прохождения через несущую стену.

Конструкция

Это устройство во многом аналогично клиентскому адаптеру. Как и последний, оно состоит из приёмопередатчика и интегрированного интерфейсного чипа, но наделено бóльшим количеством интеллектуальных функций и более сложной электроникой.

Конструктивно точки доступа могут быть выполнены как для наружного использования (защищённый от воздействий внешней среды вариант), так и для использования внутри деловых и жилых помещений. Также существуют устройства, предназначенные для промышленного использования, учитывающие специфику производства.

Что касается функциональности, у различных точек доступа она может существенно различаться, иногда предоставляя средства диагностики и контроля сети, удалённой настройки и устранения неисправностей. Кроме того, в последнее

время появились точки доступа, позволяющие производить многопользовательский обмен файлами (их трансляцию), минуя сервер.

На конец 2009 можно говорить о растущей популярности комбинированных устройств, интегрирующих в себе функции собственно беспроводного сетевого адаптера (платы, карты, контроллера), маршрутизатора и, например, кабельного модема.

Применение

Точки доступа призваны выполнять самые разнообразные функции, как для подключения группы компьютеров (каждый с беспроводным сетевым адаптером) в самостоятельные сети (режим Ad-hoc), так и для выполнения функции моста между беспроводными и кабельными участками сети (режим Infrastructure).

Для режима Ad-hoc максимально возможное количество станций - 256. В Infrastructure-режиме допустимо до 2048 беспроводных узлов.

Следует учитывать, что точка доступа - это обычный концентратор. При нескольких подключениях к одной точке полоса пропускания делится на количество подключённых пользователей. Теоретически ограничений на количество подключений нет, но на практике стоит ограничиться, исходя из минимально необходимой скорости передачи данных для каждого пользователя.

С помощью точки доступа можно легко организовать **роуминг** при перемещении мобильного компьютера пользователя в зоне охвата большей, чем зона охвата одной точки доступа, организовав «соты» из нескольких точек доступа и обеспечив перекрытие их зон действия. В этом случае необходимо обеспечить, чтобы в предполагаемой зоне перемещения мобильного пользователя все точки доступа и мобильные компьютеры имели одинаковые настройки (номера каналов, идентификаторы и др.).

Пример применения

Использование беспроводной точки доступа и мобильного компьютера. Если вам требуется не только объединить компьютеры в беспроводную сеть, но и соединить этот сегмент сети с проводным, то самый простой способ - установка так называемой «точки доступа». При использовании точки доступа вы

фактически имеете выделенное сетевое устройство, работа которого не зависит ни от загруженности других ПК, ни от их конфигурации, что является несомненным плюсом. Вам не придётся выполнять настройки сложного программного обеспечения или опасаться, что компьютер окажется в очередной раз выключенным, а необходимая служба не будет запущена.

Усиление сигнала

Репитер WiFi (вайлес фиделати) «беспроводное качество» или «беспроводная точность».

Это усилитель WiFi, работающий по принципу ретранслятора сигнала. Репитер позволяет расширить существующую WiFi-сеть. Он принимает сигнал WiFi и передает его дальше.

устанавливается в помещении; расширяет зону покрытия на 15-20 метров;

Стандарты

Самыми популярными стандартами для точек доступа являются Wi-Fi (IEEE 802.11) и Bluetooth. В технологии Bluetooth существует специальный профиль PAN (Personal Area Network) для этих целей.

7.Wi-Fi

Wi-Fi - (Wireless Fidelity (вайлес фиделати) «беспроводное качество» или «беспроводная точность») так называют один из стандартов беспроводной передачи данных, а точнее, стандарт IEEE 802.11b. Он входит в группу из 8 стандартов беспроводной передачи данных, из которых технически реализованы только два - 802.11a и 802.11b.

На самом деле все спецификации Wi-Fi являются стандартом в стандарте. С одной стороны, они все должны удовлетворять стандарту беспроводных сетей 802.11, а с другой – они входят в состав крупнейшего стандарта локальных сетей IEEE 802. И преимущества такого подхода сложно недооценивать. Так, спецификации 802.11 затрагивают лишь два нижних уровня (физический и канальный) общей модели ISO/OSI, состоящей из семи уровней. На практике это означает, что любое приложение, равно как и операционная система, не

почувствует никакой разницы, будет ли оно работать, например, в проводной локальной сети Ethernet, или беспроводной Wi-Fi, а следовательно, затраты на переход с проводной технологии на беспроводную будут определяться лишь стоимостью оборудования и его установки, и никакая разработка и замена программного обеспечения не потребуется.

Оборудование, предназначенное для работы в стандарте 802.11, в основном делится на два класса – это **клиенты и точки доступа** (Access Point). Роль **клиентов** могут играть настольные компьютеры, ноутбуки, КПК, телефоны, принтеры, игровые приставки и прочая портативная и стационарная бытовая техника, оборудованная Wi-Fi-модулем. Если в ПК или КПК изначально отсутствует поддержка беспроводных сетей, то в большинстве случаев это можно с легкостью восполнить приобретением соответствующего адаптера, который может быть реализован в форме практически любой платы расширения. **Точки доступа** обычно выполнены в виде отдельного внешнего устройства, подключаемого непосредственно к кабелю проводной сети Ethernet или к любому другому совместимому источнику широкополосного доступа в Интернет. Иногда точки доступа комбинируют с каким-либо другим устройством, например, весьма распространены ADSL-модемы, совмещенные с точкой доступа Wi-Fi. На точку доступа возлагается львиная часть работы по обслуживанию беспроводной сети: она должна не только поддерживать радиопередачу со всеми клиентами и связывать сеть с внешним миром, но и регулировать трафик, обрабатывать данные и совершать массу других операций. Также в некоторых случаях может потребоваться и дополнительное оборудование: например, при недостаточном уровне сигнала нужны антенны, а при необходимости соединения между собой двух сетей – мосты.

Существует **два основных способа организации беспроводной сети** – это клиент-сервер (Infrastructure Mode) и точка-точка (Ad-hoc). В первом случае сеть состоит из одной или нескольких точек доступа и произвольного количества клиентов. Это стандартная модель построения локальной сети, которая принципиально отличается от проводной разве что отсутствием тех самых

проводов. Во втором случае связь устанавливается непосредственно между несколькими клиентами, минуя точку доступа. Такая модель удобна для соединения между собой нескольких портативных устройств, например, для моментальной печати фотографий с Wi-Fi-камеры на Wi-Fi-принтер или многопользовательской игры на портативных консолях (Sony PSP, Nintendo DS и других).

Wi-Fi - торговая марка Wi-Fi Alliance для беспроводных сетей на базе стандарта IEEE 802.11. Под аббревиатурой Wi-Fi (от английского словосочетания Wireless Fidelity (вайлес фиделати), которое можно дословно перевести как «беспроводное качество» или «беспроводная точность») в настоящее время развивается целое семейство стандартов передачи цифровых потоков данных по радиоканалам.

Любое оборудование, соответствующее стандарту IEEE 802.11, может быть протестировано в Wi-Fi Alliance и получить соответствующий сертификат и право нанесения логотипа Wi-Fi.

Происхождение названия

Термин «Wi-Fi» изначально был придуман как игра слов для привлечения внимания потребителя «намёком» на Hi-Fi (англ. *High Fidelity* (фиделати) - высокая точность). Несмотря на то, что поначалу в некоторых пресс-релизах WESA фигурировало словосочетание «Wireless Fidelity» («беспроводная точность»), на данный момент от такой формулировки отказались, и термин «Wi-Fi» никак не расширяется.

Принцип работы

Обычно схема Wi-Fi сети содержит не менее одной точки доступа и не менее одного клиента. Также возможно подключение двух клиентов в режиме точка-точка (Ad-hoc), когда точка доступа не используется, а клиенты соединяются посредством сетевых адаптеров «напрямую». Точка доступа передаёт свой идентификатор сети (SSID русск.) с помощью специальных сигнальных пакетов на скорости 0,1 Мбит/с каждые 100 мс. Поэтому 0,1 Мбит/с - наименьшая скорость передачи данных для Wi-Fi. Зная SSID сети, клиент может выяснить, возможно ли подключение к данной точке доступа. При попадании в зону действия двух точек доступа с идентичными SSID приёмник может выбирать между ними на основании данных об уровне сигнала. Стандарт Wi-Fi даёт клиенту полную свободу при выборе критериев для соединения. Более подробно принцип работы описан в официальном тексте стандарта.

Однако, стандарт не описывает всех аспектов построения беспроводных локальных сетей Wi-Fi. Поэтому каждый производитель оборудования решает эту задачу по-своему, применяя те подходы, которые он считает наилучшими с той или иной точки зрения. Поэтому возникает необходимость **классификации способов построения беспроводных локальных сетей**.

По способу объединения точек доступа в единую систему можно выделить:

- Автономные точки доступа (называются также самостоятельные, децентрализованные, умные)
 - Точки доступа, работающие под управлением контроллера (называются также «легковесные», централизованные)
 - Бесконтроллерные, но не автономные (управляемые без контроллера)
- По способу организации и управления радиоканалами можно выделить беспроводные локальные сети:
- Со статическими настройками радиоканалов
 - С динамическими (адаптивными) настройками радиоканалов
 - Со «слоистой» или многослойной структурой радиоканалов

Преимущества Wi-Fi

Беспроводной Интернет на пляже

- Позволяет развернуть сеть без прокладки кабеля, что может уменьшить стоимость развёртывания и/или расширения сети. Места, где нельзя проложить кабель, например, вне помещений и в зданиях, имеющих историческую ценность, могут обслуживаться беспроводными сетями.
- Позволяет иметь доступ к сети мобильным устройствам.
- Wi-Fi устройства широко распространены на рынке. Гарантируется совместимость оборудования благодаря обязательной сертификации оборудования с логотипом Wi-Fi.
- Мобильность. Вы больше не привязаны к одному месту и можете пользоваться Интернетом в комфортной для вас обстановке.
- В пределах Wi-Fi зоны в сеть Интернет могут выходить несколько пользователей с компьютеров, ноутбуков, телефонов и т. д.
- Излучение от Wi-Fi устройств в момент передачи данных на порядок (в 10 раз) меньше, чем у сотового телефона.

Недостатки Wi-Fi

- В диапазоне 2,4 GHz работает множество устройств, таких как устройства, поддерживающие Bluetooth, и др, и даже микроволновые печи, что ухудшает электромагнитную совместимость.
- Производителями оборудования указывается скорость на L1 (OSI), в результате чего создаётся иллюзия, что производитель оборудования завышает скорость, но на самом деле в Wi-Fi весьма высоки служебные «накладные расходы». Получается, что скорость передачи данных на L2 (OSI) в Wi-Fi сети всегда ниже заявленной скорости на L1 (OSI). Реальная скорость зависит от доли служебного трафика, которая зависит уже от наличия между устройствами физических преград (мебель, стены), наличия помех от других беспроводных устройств или электронной аппаратуры, расположения устройств относительно друг друга и т. п.
- Частотный диапазон и эксплуатационные ограничения в различных странах не одинаковы. Во многих европейских странах разрешены два дополнительных канала, которые запрещены в США; В Японии есть ещё один канал в верхней части диапазона, а другие страны, например Испания, запрещают использование низкочастотных каналов. Более того, некоторые страны, например Россия, Белоруссия и Италия, требуют регистрации всех сетей Wi-Fi, работающих

вне помещений, или требуют регистрации Wi-Fi-оператора.

- Как было упомянуто выше — в России точки беспроводного доступа, а также адаптеры Wi-Fi с ЭИИМ, превышающей 100 мВт (20 дБм), подлежат обязательной регистрации.

- Стандарт шифрования WEP может быть относительно легко взломан даже при правильной конфигурации (из-за слабой стойкости алгоритма). Новые устройства поддерживают более совершенные протоколы шифрования данных WPA и WPA2. Принятие стандарта IEEE 802.11i (WPA2) в июне 2004 года сделало возможным применение более безопасной схемы связи, которая доступна в новом оборудовании. Обе схемы требуют более стойкий пароль, чем те, которые обычно назначаются пользователями. Многие организации используют дополнительное шифрование (например VPN) для защиты от вторжения. На данный момент основным методом взлома WPA2 является подбор пароля, поэтому рекомендуется использовать сложные цифро-буквенные пароли для того, чтобы максимально усложнить задачу подбора пароля.

- В режиме точка-точка (Ad-hoc) стандарт предписывает лишь реализовать скорость 11 Мбит/сек (802.11b). Шифрование WPA(2) недоступно, только легковзламываемый WEP.

8.Модемы

Модём (акроним, составленный из слов модулятор и демодулятор) - устройство, применяющееся в системах связи для физического сопряжения информационного сигнала со средой его распространения, где он не может существовать без адаптации.

Модулятор в модеме осуществляет модуляцию (Модуляция (лат. *modulatio* — *размеренность, ритмичность*) — процесс изменения одного или нескольких параметров высокочастотного несущего колебания по закону низкочастотного информационного сигнала (сообщения). Передаваемая информация заложена в управляющем (модулирующем) сигнале, а роль переносчика информации выполняет высокочастотное колебание, называемое несущим. Модуляция, таким образом, представляет собой процесс «посадки» информационного колебания на заведомо известную несущую) несущего сигнала при передаче данных, то есть изменяет его характеристики в соответствии с изменениями входного информационного сигнала, демодулятор осуществляет обратный процесс при приёме данных из канала связи. Модем выполняет функцию окончного оборудования линии связи. Само формирование данных для передачи и обработки принимаемых данных осуществляет т. н. терминальное оборудование (в его роли может выступать и персональный компьютер).

Модемы широко применяются для связи компьютеров через телефонную сеть (*телефонный модем*), кабельную сеть (*кабельный модем*), радиоволны (en:Packet_radio, радиорелейная связь). Ранее модемы применялись также в

сотовых телефонах (пока не были вытеснены цифровыми способами передачи данных).

Виды компьютерных модемов

Модемы различаются по исполнению (внешние или внутренние), по принципу работы (аппаратные или программные), по типу сети, к которой производится подключение, а также по поддерживаемым протоколам передачи данных.

Наибольшее распространение получили внутренние программные, внешние аппаратные и встроенные модемы.

По исполнению

- *внешние* - подключаются через COM-, LPT-^Ш, USB- или Ethernet-порт, обычно имеют отдельный блок питания (существуют и USB-модемы с питанием от шины USB).

- *внутренние* - дополнительно устанавливаются внутрь системного блока или ноутбука (в слот ISA, PCI, PCI-E, PCMCIA, AMR/CNR).

- *встроенные* - являются частью устройства, куда встроены (материнской платы, ноутбука или док-станции).

По принципу работы

- *аппаратные* - все операции преобразования сигнала, поддержка физических протоколов обмена производятся встроенным в модем вычислителем (например, с использованием DSP или микроконтроллера). Также в аппаратном модеме присутствует ПЗУ, в котором записана микропрограмма, управляющая модемом.

- *программные* (софт-модемы, host based soft-modem) - все операции по кодированию сигнала, контролю ошибок и управлению протоколами реализованы программно и производятся центральным процессором компьютера. В модеме находятся только входные/выходные аналоговые цепи и преобразователи (ЦАП и АЦП), а также контроллер интерфейса (например USB).

- *полупрограммные* (controller based soft-modem) - модемы, в которых *часть* функций модема выполняет компьютер, к которому подключён модем.

По типу сети и соединения

- Модемы для телефонных линий:
 - Модемы для коммутируемых телефонных линий - наиболее распространённый в XX веке и 2000-х годах тип модемов. Используют коммутируемый удалённый доступ.
 - ISDN - модемы для цифровых коммутируемых телефонных линий.
 - DSL - используются для организации выделенных (некоммутируемых) линий средствами обычной телефонной сети. Отличаются от коммутируемых модемов тем, что используют другой частотный диапазон, а также тем, что по телефонным линиям сигнал передается только до АТС. Обычно позволяют одновременно с обменом данными осуществлять использование телефонной линии для переговоров.
- Кабельные модемы - используются для обмена данными по специализированным кабелям - к примеру, через кабель коллективного телевидения по протоколу DOCSIS.
- Радиомодемы - работают в радиодиапазоне, используют собственные наборы частот и протоколы:
 - Беспроводные модемы - работают по протоколам сотовой связи (GPRS, EDGE, 3G, LTE) или Wi-Fi. Часто имеют исполнения в виде USB-брелока. В качестве таких модемов также часто используют терминалы мобильной связи.
 - Спутниковые модемы - используются для организации спутникового Интернета. Принимают и обрабатывают сигнал, полученный со спутника.
- PowerLine-модемы (стандарт HomePlug) - используют технологию передачи данных по проводам бытовой электрической сети.

Устройство

Плата модема *Acorp Sprinter@ADSL LAN120M*

1. **Порты ввода-вывода** - схемы, предназначенные для обмена данными между телефонной линией и модемом с одной стороны, и модемом и компьютером - с другой. Для взаимодействия с аналоговой телефонной линией зачастую используется трансформатор.

2. **Сигнальный процессор** (Digital Signal Processor, DSP) Обычно модулирует исходящие сигналы и демодулирует входящие на цифровом уровне в соответствии с используемым протоколом передачи данных. Может также

выполнять другие функции.

3. Контроллер управляет обменом с компьютером. **Контроллер** ([англ. controller](#) — регулятор, управляющее устройство).

4. Микросхемы памяти:

- ROM - энергонезависимая память, в которой хранится микропрограмма управления модемом - прошивка, которая включает в себя наборы команд и данных для управления модемом, все поддерживаемые коммуникационные протоколы и интерфейс с компьютером. Обновление прошивки модема доступно в большинстве современных моделей, для чего служит специальная процедура, описанная в руководстве пользователя. Для обеспечения возможности перепрошивки для хранения микропрограмм применяется флэш-память (EEPROM). Флэш-память позволяет легко обновлять микропрограмму модема, исправляя ошибки разработчиков и расширяя возможности устройства. В некоторых моделях внешних модемов она так же используется для записи входящих голосовых и факсимильных сообщений при выключенном компьютере.

- NVRAM - энергонезависимая электрически перепрограммируемая память, в которой хранятся настройки модема (профиль модема). Пользователь может изменять установки, например, используя набор AT-команд.

- RAM - оперативная память модема, используется для буферизации принимаемых и передаваемых данных, работы алгоритмов сжатия и прочего.

Дополнительные функции

Факс-модем - позволяет компьютеру, к которому он присоединён, передавать и принимать факсимильные изображения на другой факс-модем или обычный факс-аппарат.

Голосовой модем - с функцией оцифровки сигнала с телефонной линии и воспроизведения произвольного звука в линию. Часть голосовых модемов имеет встроенный микрофон. Такой модем позволяет осуществить:

- передачу голосовых сообщений в режиме реального времени на другой удалённый голосовой модем, приём сообщений от него и воспроизведение их через внутренний динамик;

- использование в режиме автоответчика и для организации голосовой почты.

Сетевые адаптеры

Ада́птер ([англ.](#) *adapter*, от [лат.](#) *adapto* - приспособляю) - приспособление, устройство или деталь, предназначенные для соединения устройств, не имеющих иного совместимого способа соединения.

Сетевые адаптеры или NIC (Network Interface Card) - это сетевое оборудование, обеспечивающее функционирование сети на физическом и канальном уровнях.

Сетевой адаптер (Network Interface Card, NIC) - это периферийное устройство компьютера, непосредственно взаимодействующее со средой передачи данных, которая прямо или через другое коммуникационное оборудование связывает его с другими компьютерами. Это устройство решает задачи надежного обмена двоичными данными, представленными соответствующими электромагнитными сигналами, по внешним линиям связи. Как и любой контроллер (управляющее устройство) компьютера, сетевой адаптер работает под управлением драйвера операционной системы и распределение функций между сетевым адаптером и драйвером может изменяться от реализации к реализации.

В первых локальных сетях сетевой адаптер с сегментом коаксиального кабеля представлял собой весь спектр коммуникационного оборудования, с помощью которого организовывалось взаимодействие компьютеров. Сетевой адаптер компьютера-отправителя непосредственно по кабелю взаимодействовал с сетевым адаптером компьютера-получателя. В большинстве современных стандартов для локальных сетей предполагается, что между сетевыми адаптерами взаимодействующих компьютеров устанавливается специальное коммуникационное устройство (концентратор, мост, коммутатор или маршрутизатор), которое берет на себя некоторые функции по управлению потоком данных.

Сетевой адаптер обычно выполняет следующие функции:

- Оформление передаваемой информации в виде кадра определенного формата. Кадр включает несколько служебных полей, среди которых имеется

адрес компьютера назначения и контрольная сумма кадра, по которой сетевой адаптер станции назначения делает вывод о корректности доставленной по сети информации.

- Получение доступа к среде передачи данных. В локальных сетях в основном применяются разделяемые между группой компьютеров каналы связи (общая шина, кольцо), доступ к которым предоставляется по специальному алгоритму (наиболее часто применяются метод случайного доступа или метод с передачей маркера доступа по кольцу). В последних стандартах и технологиях локальных сетей наметился переход от использования разделяемой среды передачи данных к использованию индивидуальных каналов связей компьютера с коммуникационными устройствами сети, как это всегда делалось в телефонных сетях, где телефонный аппарат связан с коммутатором АТС индивидуальной линией связи. Технологиями, использующими индивидуальные линии связи, являются 100VG-AnyLAN, ATM и коммутирующие модификации традиционных технологий - switching Ethernet, switching Token Ring и switching FDDI. При использовании индивидуальных линий связи в функции сетевого адаптера часто входит установление соединения с коммутатором сети.

- Кодирование последовательности бит кадра последовательностью электрических сигналов при передаче данных и декодирование при их приеме. Кодирование должно обеспечить передачу исходной информации по линиям связи с определенной полосой пропускания и определенным уровнем помех таким образом, чтобы принимающая сторона смогла распознать с высокой степенью вероятности посланную информацию. Так как в локальных сетях используются широкополосные кабели, то сетевые адаптеры не используют модуляцию сигнала, необходимую для передачи дискретной информации по узкополосным линиям связи (например, телефонным каналам тональной частоты), а передают данные с помощью импульсных сигналов. Представление же двоичных 1 и 0 может быть различным.

- Преобразование информации из параллельной формы в последовательную и обратно. Эта операция связана с тем, что для упрощения

проблемы синхронизации сигналов и удешевления линий связи в вычислительных сетях информация передается в последовательной форме, бит за битом, а не побайтно, как внутри компьютера.

- Синхронизация битов, байтов и кадров. Для устойчивого приема передаваемой информации необходимо поддержание постоянного синхронизма приемника и передатчика информации. Сетевой адаптер использует для решения этой задачи специальные методы кодирования, не использующие дополнительной шины с тактовыми синхросигналами. Эти методы обеспечивают периодическое изменение состояния передаваемого сигнала, которое используется тактовым генератором приемника для подстройки синхронизма. Кроме синхронизации на уровне битов, сетевой адаптер решает задачу синхронизации и на уровне байтов, и на уровне кадров.

Сетевые адаптеры различаются по типу и разрядности используемой в компьютере внутренней шины данных - ISA, EISA, PCI, MCA.

Сетевые адаптеры различаются также **по типу принятой** в сети сетевой технологии - Ethernet, Token Ring, FDDI и т.п. Как правило, конкретная модель сетевого адаптера работает по определенной сетевой технологии (например, Ethernet). В связи с тем, что для каждой технологии сейчас имеется возможность использования различных сред передачи данных (тот же Ethernet поддерживает коаксиальный кабель, неэкранированную витую пару и оптоволоконный кабель), сетевой адаптер может поддерживать как одну, так и одновременно несколько сред. В случае, когда сетевой адаптер поддерживает только одну среду передачи данных, а необходимо использовать другую, применяются трансиверы и конверторы.

Трансивер (приемопередатчик, **transmitter+receiver**) - это часть сетевого адаптера, его оконечное устройство, выходящее на кабель. В первом стандарте Ethernet, работающем на толстом коаксиале, трансивер располагался непосредственно на кабеле и связывался с остальной частью адаптера, располагавшейся внутри компьютера, с помощью интерфейса AUI (attachment unit interface). В других вариантах Ethernet'a оказалось удобным выпускать сетевые

адаптеры (да и другие коммуникационные устройства) с портом AUI, к которому можно присоединить трансивер для требуемой среды.

Вместо подбора подходящего трансивера можно использовать *конвертор*, который может согласовать выход приемопередатчика, предназначенного для одной среды, с другой средой передачи данных (например, выход на витую пару преобразуется в выход на коаксиальный кабель).

Концентратор, коммутаторы

Сетевой концентратор или **хаб** (от англ. *hub* - центр) - устройство для объединения компьютеров в сеть Ethernet с применением кабельной инфраструктуры типа *витая пара*. В настоящее время вытеснены сетевыми коммутаторами.

Сетевые концентраторы также могли иметь разъёмы для подключения к существующим сетям на базе толстого или тонкого коаксиального кабеля.

Принцип работы

Концентратор работает на первом (физическом) уровне сетевой модели OSI, ретранслируя входящий сигнал с одного из портов в сигнал на все остальные (подключённые) порты, реализуя, таким образом, свойственную Ethernet топологию *общая шина*, с разделением пропускной способности сети между всеми устройствами и работой в режиме полудуплекса. Коллизии (то есть попытка двух и более устройств начать передачу одновременно) обрабатываются аналогично сети Ethernet на других носителях - устройства самостоятельно прекращают передачу и возобновляют попытку через случайный промежуток времени, говоря современным языком, концентратор объединяет устройства в одном домене коллизий.

Сетевой концентратор также обеспечивает бесперебойную работу сети при отключении устройства от одного из портов или повреждении кабеля, в отличие, например, от сети на коаксиальном кабеле, которая в таком случае прекращает работу целиком.

Сетевой коммутатор (жарг. **свич** от англ. *switch* - переключатель) - устройство, предназначенное для соединения нескольких узлов компьютерной сети в пределах одного или нескольких сегментов сети. Коммутатор работает на канальном (втором) уровне модели OSI. Коммутаторы были разработаны с использованием мостовых технологий и часто рассматриваются как многопортовые мосты. Для соединения нескольких сетей на основе сетевого уровня служат маршрутизаторы.

В отличие от концентратора, который распространяет трафик (**Сетевой трафик** или **Интернет-трафик** (англ. *Traffic* — «движение», «грузооборот») — объём информации, передаваемой через компьютерную сеть за определенный период времени. Количество трафика измеряется как в пакетах, так и в битах, байтах и их производных: килобайт (Кб), мегабайт (Мб) и т. д. Трафик различают на: входящий (информация, поступающая из сети); исходящий (информация, поступающая в сеть); внутренний (в пределах определенной сети, чаще всего локальной); внешний (за пределами определенной сети, чаще всего — интернет-трафик). от одного подключенного устройства ко всем остальным, **коммутатор** передаёт данные только непосредственно получателю (исключение составляет широковещательный трафик всем узлам сети и трафик для устройств, для которых не известен исходящий порт коммутатора). Это повышает производительность и безопасность сети, избавляя остальные сегменты сети от необходимости (и возможности) обрабатывать данные, которые им не предназначались.

Режимы коммутации

Существует три способа коммутации. Каждый из них - это комбинация таких параметров, как время ожидания и надёжность передачи.

1. С промежуточным хранением (Store and Forward). Коммутатор читает всю информацию в кадре, проверяет его на отсутствие ошибок, выбирает порт коммутации и после этого посылает в него кадр.

2. Сквозной (cut-through). Коммутатор считывает в кадре только адрес назначения и после выполняет коммутацию. Этот режим уменьшает задержки при передаче, но в нём нет метода обнаружения ошибок.

3. Бесфрагментный (fragment-free) или *гибридный*. Этот режим является

модификацией сквозного режима. Передача осуществляется после фильтрации фрагментов коллизий (первые 64 байта кадра анализируются на наличие ошибки и при её отсутствии кадр обрабатывается в сквозном режиме).

Задержка, связанная с «принятием коммутатором решения», добавляется к времени, которое требуется кадру для входа на порт коммутатора и выхода с него, и вместе с ним определяет общую задержку коммутатора.

Симметричная и асимметричная коммутация

Свойство симметрии при коммутации позволяет дать характеристику коммутатора с точки зрения ширины [полосы пропускания](#) (**Полоса пропускания (прозрачности)**) - диапазон [частот](#), в пределах которого [амплитудно-частотная характеристика](#) (АЧХ) акустического, радиотехнического, оптического или механического устройства достаточно равномерна для того, чтобы обеспечить передачу [сигнала](#) без существенного искажения его формы. Ширина полосы пропускания - полоса частот, в пределах которой неравномерность частотной характеристики не превышает заданной) для каждого его [порта](#). Симметричный коммутатор обеспечивает коммутируемые соединения между портами с одинаковой шириной полосы пропускания, например, когда все порты имеют ширину пропускания 10 [Мб/с](#) или 100 Мб/с.

Асимметричный коммутатор обеспечивает коммутируемые соединения между портами с различной шириной полосы пропускания, например, в случаях комбинации портов с шириной полосы пропускания 10 Мб/с и 100 Мб/с или 100 Мб/с и 1000 Мб/с.

Асимметричная коммутация используется в случае наличия больших сетевых потоков типа [клиент-сервер](#), когда многочисленные пользователи обмениваются информацией с сервером одновременно, что требует большей ширины пропускания для того порта коммутатора, к которому подсоединен сервер, с целью предотвращения переполнения на этом порте. Для того чтобы направить поток данных с порта 100 Мб/с на порт 10 Мб/с без опасности переполнения на последнем, асимметричный коммутатор должен иметь буфер памяти.

Асимметричный коммутатор также необходим для обеспечения большей

ширины полосы пропускания каналов между коммутаторами, осуществляемых через вертикальные кросс-соединения, или каналов между сегментами магистрали.

Буфер памяти

Для временного хранения фреймов и последующей их отправки по нужному адресу коммутатор может использовать буферизацию. Буферизация может быть также использована в том случае, когда порт пункта назначения занят. **Буфером называется** область памяти, в которой коммутатор хранит передаваемые данные.

Буфер памяти может использовать два метода хранения и отправки фреймов: **Фрейм** — ([англ. frame](#) — «каркас» или «рамка») — способ представления знаний в [искусственном интеллекте](#), представляющий собой схему действий в реальной ситуации. Первоначально термин «фрейм» ввёл [Марвин Минский](#) в 70-е годы XX века для обозначения структуры знаний для восприятия пространственных сцен. **Фрейм** — это модель абстрактного образа, минимально возможное описание сущности какого-либо объекта, явления, события, ситуации, процесса.

Фреймы используются в системах искусственного интеллекта (например, в экспертных системах) как одна из распространенных форм представления знаний.

буферизация по портам и буферизация с общей памятью. При буферизации по портам пакеты хранятся в очередях (queue), которые связаны с отдельными входными портами. Пакет передается на выходной порт только тогда, когда все фреймы, находившиеся впереди него в очереди, были успешно переданы. При этом возможна ситуация, когда один фрейм задерживает всю очередь из-за занятости порта его пункта назначения. Эта задержка может происходить даже в том случае, когда остальные фреймы могут быть переданы на открытые порты их пунктов назначения.

При буферизации в общей памяти все фреймы хранятся в общем буфере памяти, который используется всеми портами коммутатора. Количество памяти, отводимой порту, определяется требуемым ему количеством. Такой метод называется динамическим распределением буферной памяти. После этого фреймы, находившиеся в буфере, динамически распределяются выходным портам. Это позволяет получить фрейм на одном порте и отправить его с другого порта, не устанавливая его в очередь.

Коммутатор поддерживает карту портов, в которые требуется отправить фреймы. Очистка этой карты происходит только после того, как фрейм успешно

отправлен.

Поскольку память буфера является общей, размер фрейма ограничивается всем размером буфера, а не долей, предназначенной для конкретного порта. Это означает, что крупные фреймы могут быть переданы с меньшими потерями, что особенно важно при асимметричной коммутации, то есть когда порт с шириной полосы пропускания 100 Мб/с должен отправлять пакеты на порт 10 Мб/с.

Возможности и разновидности коммутаторов

Коммутаторы подразделяются на управляемые и неуправляемые (наиболее простые).

Более сложные коммутаторы позволяют управлять коммутацией на сетевом (третьем) уровне модели OSI. Обычно их именуют соответственно, например «Layer 3 Switch» или сокращенно «L3 Switch». Управление коммутатором может осуществляться посредством Web-интерфейса, протокола SNMP, RMON и т. п.

Многие управляемые коммутаторы позволяют настраивать дополнительные функции: VLAN, QoS, агрегирование, зеркалирование.

Сложные коммутаторы можно объединять в одно логическое устройство — стек — с целью увеличения числа портов. Например, можно объединить 4 коммутатора с 24 портами и получить логический коммутатор с 90 $((4*24)-6=90)$ портами либо с 96 портами (если для стекирования используются специальные порты).

Повторители

Повторитель (репíтер, от англ. repeater) - сетевое оборудование, предназначенное для увеличения расстояния сетевого соединения путём повторения электрического сигнала «один в один». Бывают однопортовые повторители и многопортовые. В терминах модели OSI работает на физическом уровне.

Одной из первых задач, которая стоит перед любой технологией транспортировки данных, является возможность их передачи на максимально

большое расстояние. Физическая среда накладывает на этот процесс своё ограничение - рано или поздно мощность сигнала падает, и приём становится невозможным. Но ещё большее значение имеет то, что искажается «форма сигнала» - закономерность, в соответствии с которой мгновенное значение уровня сигнала изменяется во времени. Это происходит в результате того, что провода, по которым передаётся сигнал, имеют собственную ёмкость и индуктивность. Электрические и магнитные поля одного проводника наводят ЭДС в других проводниках (длинная линия).

Привычное для аналоговых систем усиление не годится для высокочастотных цифровых сигналов. Разумеется, при его использовании какой-то небольшой эффект может быть достигнут, но с увеличением расстояния искажения быстро нарушат целостность данных.

Проблема не нова, и в таких ситуациях применяют не усиление, а повторение сигнала. При этом устройство на входе должно принимать сигнал, далее распознавать его первоначальный вид, и генерировать на выходе его точную копию. Такая схема в теории может передавать данные на сколь угодно большие расстояния (если не учитывать особенности разделения физической среды в Ethernet).

Первоначально в Ethernet использовался коаксиальный кабель с топологией «шина», и нужно было соединять между собой всего несколько протяжённых сегментов. Для этого обычно использовались повторители (repeater), имевшие два порта. Несколько позже появились многопортовые устройства, называемые концентраторами (concentrator). Их физический смысл был точно такой же, но восстановленный сигнал транслировался на все активные порты, кроме того, с которого пришёл сигнал.

С появлением протокола 10baseT (витой пары) для избежания терминологической путаницы многопортовые повторители для витой пары стали называться сетевыми концентраторами (хабами), а коаксиальные — повторителями (репитерами), по крайней мере, в русскоязычной литературе. Эти названия хорошо прижились и используются в настоящее время очень широко.

Институт инженеров по электротехнике и электронике - IEEE

Институт инженеров по электротехнике и электронике - IEEE (англ. *Institute of Electrical and Electronics Engineers*) (I triple E - «Ай трипл и») - международная некоммерческая ассоциация специалистов в области техники, мировой лидер в области разработки стандартов по радиоэлектронике и электротехнике.

Эта общественная некоммерческая ассоциация профессионалов появилась в 1963 году, в результате слияния Института радиотехников (англ. *Institute of Radio Engineers*, IRE) созданном в 1912 году и Американского института инженеров-электриков (англ. *American Institute of Electrical Engineers*, AIEE) созданном в 1884 году. IEEE объединяет более 400000 индивидуальных членов из 170 стран, в том числе более 100000 студентов, издаёт третью часть мировой технической литературы, касающейся применения радиоэлектроники, компьютеров, систем управления, электротехники, в том числе (январь 2011) 122 реферируемых научных журнала и 36 отраслевых журналов для специалистов, проводит в год более 300 крупных конференций, принимала участие в разработке около 900 действующих стандартов.

Главная цель IEEE - информационная и материальная поддержка специалистов для организации и развития научной деятельности в электротехнике, электронике, компьютерной технике и информатике, приложение их результатов для пользы общества, а также профессиональный рост членов IEEE. Получение бесценной информации о новейших исследованиях и разработках в радиоэлектронике и электротехнике возможно только благодаря IEEE.

В России действует Сибирская, Северо-Западная (Санкт-Петербург) и Центральная Российская (Москва) секции. В составе Сибирской секции, занимающей самую большую в мире территорию, находится восемь научных групп различных обществ IEEE и семь студенческих отделений, в составе

Российской секции - 15 групп и два студенческих отделения. Общее число членов IEEE по России - примерно 1800 чел., включая студентов. В Сибирской секции работает группа молодых инженеров (GOLD, Graduates of the Last Decade), группа "Женщины в инженерной деятельности" и ассоциация связи с промышленностью. Членство в IEEE очень престижно и доступно каждому. Подробнее об Институте на русском языке можно узнать из материалов сайтов Томской группы IEEE <http://ieeetomsk.ru/ru/index.htm> и <http://chapters.comsoc.org/tomsk>

Северо-Западная Секция IEEE в Санкт-Петербурге представлена основной секцией (<http://ieeespbrussia.org/>), включающей в себя большое количество научных групп, а также тремя студенческими секциями:

- Студенческая Секция IEEE на Северо-Западе России при СПбГЭТУ ЛЭТИ им. Ульянова-Ленина (<http://ieeernw.ru>)

- Студенческая Секция IEEE на Северо-Западе России при СПбНИУ ИТМО

- Студенческая Секция IEEE на Северо-Западе России при СПбГУКиТ

- IEEE 754 - числа с плавающей запятой

- **IEEE 802 - семейство стандартов IEEE, касающихся локальных вычислительных сетей (LAN) и сетей мегаполисов (MAN)**

- IEEE 1003 - POSIX - Стандарт совместимости UNIX-подобных ОС

- IEEE 1059 - Guide for Software Verification and Validation Plans - Руководство по планированию верификации и подтверждения достоверности программного обеспечения.

- IEEE 1063 - «IEEE Standard for Software User Documentation» - Стандарт руководства пользователя для программного обеспечения.

- IEEE 1149 - Стандарт периферийного сканирования микросхем (Boundary Scan) - тестирование, программирование и локализация неисправностей печатных плат.

- IEEE 1284 - параллельный интерфейс

- IEEE 1294 - USB

- IEEE 1394 - FireWire(i-Link) - последовательная высокоскоростная шина, предназначенная для обмена цифровой информацией между компьютером и

другими электронными устройствами.

- IEEE 1667 - Standard Protocol for Authentication in Host Attachments of Transient Storage Devices - Стандартный протокол аутентификации при подключении съемных устройств хранения данных.

- IEEE 1990 - Функциональный язык программирования Scheme.

Перейти к: навигация, поиск

IEEE 802 - группа стандартов семейства IEEE, касающихся локальных вычислительных сетей (LAN) и сетей мегаполисов (MAN).

В частности, стандарты IEEE 802 ограничены сетями с пакетами переменной длины. Число 802 являлось следующим свободным номером для стандарта, хотя часто ассоциируется с датой принятия стандарта - февраль 1980 года.

Службы и протоколы, указанные в IEEE 802 находятся на двух нижних уровнях (Канальный уровень и Физический) семиуровневой сетевой модели OSI. Фактически, IEEE 802 разделяет канальный уровень OSI на два подуровня - Media Access Control (MAC) и Logical Link Control LLC. Таким образом, уровни располагаются в следующем виде:

- Канальный уровень
 - Подуровень LLC
 - Подуровень MAC
- Физический уровень

Семейство стандартов IEEE 802 поддерживается комитетом по стандартам IEEE 802 LAN/MAN Standards Committee (LMSC). Наиболее часто используются для семейства Ethernet, Token Ring, беспроводной LAN, мостов и сетей с виртуальными мостами (Virtual Bridged LANs). Каждая отдельная рабочая группа работает в своей области стандарта.

Рабочие группы

название	описание	примечание
<u>IEEE 802.1</u>	Управление сетевыми устройствами и их взаимодействие	
<u>IEEE 802.2</u>	Logical Link Control (<u>LLC</u>)	не активна
<u>IEEE 802.3</u>	Технология <u>Ethernet</u>	
<u>IEEE 802.4</u>	Маркерная шина <u>Token bus</u>	расформирована
<u>IEEE 802.5</u>	Определяет MAC уровень для <u>маркерного кольца</u>	не активна
<u>IEEE 802.6</u>	Городские сети (<u>MAN</u>)	расформирована
<u>IEEE 802.7</u>	Широкополосная передача по <u>коаксиальному кабелю</u>	расформирована
<u>IEEE 802.8</u>	Волоконно-оптические сети	расформирована
<u>IEEE 802.9</u>	Интегрированные сети передачи речевых сообщений и данных	расформирована
<u>IEEE 802.10</u>	Сетевая безопасность	расформирована
<u>IEEE 802.11</u> <u>a/b/g/n</u>	Беспроводные локальные сети	
<u>IEEE 802.12</u>	Доступ по требованию с приоритетами	расформирована
<u>IEEE 802.13</u>	Использовалась для <u>100BASE-X Ethernet</u>	
<u>IEEE 802.14</u>	Кабельные модемы	расформирована
<u>IEEE 802.15</u>	<u>Беспроводные персональные сети (WPAN), Bluetooth</u>	
<u>IEEE 802.15.1</u>	<u>Bluetooth</u> сертификация	
<u>IEEE 802.15.2</u>	Существование <u>IEEE 802.15</u> и <u>IEEE 802.11</u>	
<u>IEEE 802.15.3</u>	<u>High-Rate WPAN</u> сертификация	
<u>IEEE 802.15.4</u>	Физический уровень и управление доступом к	

среде для беспроводных персональных сетей с низким уровнем скорости (Low-rate WPAN).

<u>IEEE 802.15.5</u>	Mesh networking для WPAN	
<u>IEEE 802.16</u>	Беспроводная городская сеть (<u>WiMAX</u> сертификация)	
<u>IEEE 802.16e</u>	(Мобильные) Широковещательные беспроводные сети	
<u>IEEE 802.16.1</u>	Служба местного многоточечного распределения	
<u>IEEE 802.17</u>	Эластичное кольцо пакетов	
<u>IEEE 802.18</u>	Радиорегулирование	
<u>IEEE 802.19</u>	Сосуществование сетей	
<u>IEEE 802.20</u>	Мобильный широковещательный беспроводной доступ	
<u>IEEE 802.21</u>	Media Independent Handoff	
<u>IEEE 802.22</u>	Местные беспроводные сети	
<u>IEEE 802.23</u>	Рабочая группа чрезвычайных сервисов	новая (Март, 2010)

Logical Link Control (общепринятое сокращение - **LLC**) - подуровень управления логической связью - по стандарту IEEE 802 - верхний подуровень канального уровня модели OSI, осуществляет:

- управление передачей данных;
- обеспечивает проверку и правильность передачи информации по соединению.

Структура кадра

По своему назначению все кадры уровня LLC (называемые в стандарте IEEE 802.2 блоками данных - Protocol Data Unit, PDU) подразделяются на три типа - информационные, управляющие и нумерованные:

- Информационные кадры предназначены для передачи информации в процедурах с установлением логического соединения и должны обязательно содержать поле информации. В процессе передачи информационных блоков осуществляется их нумерация в режиме скользящего окна.

- Управляющие кадры предназначены для передачи команд и ответов в процедурах с установлением логического соединения, в том числе запросов на повторную передачу искаженных информационных блоков.

- Нумерованные кадры предназначены для передачи нумерованных команд и ответов, выполняющих в процедурах без установления логического соединения передачу информации, идентификацию и тестирование LLC-уровня, а в процедурах с установлением логического соединения — установление и разъединение логического соединения, а также информирование об ошибках.

Все типы кадров уровня LLC имеют единый формат. Они содержат четыре поля:

- адрес точки входа сервиса назначения (Destination Service Access Point, DSAP),
- адрес точки входа сервиса источника (Source Service Access Point, SSAP),
- управляющее поле (Control)
- поле данных (Data)

Кадр LLC обрамляется двумя однобайтовыми полями «Флаг», имеющими значение 01111110. Флаги используются на MAC-уровне для определения границ блока. (Отметим, что формат кадров LLC, за исключением поля адреса точки входа сервиса источника, соответствует формату кадра HDLC, а также одного из вариантов протокола HDLC - протокола LAP-B, используемого в сетях X.25).

Поле данных кадра LLC предназначено для передачи по сети пакетов протоколов верхних уровней - IP, IPX, AppleTalk, DECnet, в редких случаях -

прикладных протоколов, когда те не пользуются сетевыми протоколами, а вкладывают свои сообщения непосредственно в кадры канального уровня. Поле данных может отсутствовать в управляющих кадрах и некоторых нумерованных кадрах.

Поле управления (один байт) используется для обозначения типа кадра данных — информационный, управляющий или нумерованный. Кроме этого, в этом поле указываются порядковые номера отправленных и успешно принятых кадров, если подуровень LLC работает по процедуре LLC2 с установлением соединения. Формат поля управления полностью совпадает с форматом поля управления кадра LAP-B.

Поля DSAP и SSAP позволяют указать, какой сервис верхнего уровня пересылает данные с помощью этого кадра. Программному обеспечению узлов сети при получении кадров канального уровня необходимо распознать, какой протокол вложил свой пакет в поле данных поступившего кадра, для того, чтобы передать извлеченный из кадра пакет нужному протоколу для последующей обработки. Например, в качестве значения DSAP и SSAP может выступать код протокола IPX или же код протокола покрывающего дерева Spanning Tree.

У этого термина существуют и другие значения, см. MAC.

MAC-адрес (от англ. *Media Access Control* - управление доступом к среде, также **Hardware Address**) - это уникальный идентификатор, присваиваемый каждой единице оборудования компьютерных сетей. Большинство сетевых протоколов канального уровня используют одно из трёх пространств MAC-адресов, управляемых IEEE: MAC-48, EUI-48 и EUI-64. Адреса в каждом из пространств теоретически должны быть глобально уникальными. Не все протоколы используют MAC-адреса, и не все протоколы, использующие MAC-адреса, нуждаются в подобной уникальности этих адресов.

В широковещательных сетях (таких, как сети на основе Ethernet) MAC-адрес позволяет уникально идентифицировать каждый узел сети и доставлять данные только этому узлу. Таким образом, MAC-адреса формируют основу сетей

на канальном уровне, которую используют протоколы более высокого (сетевого) уровня. Для преобразования MAC-адресов в адреса сетевого уровня и обратно применяются специальные протоколы (например, ARP и RARP в сетях IPv4 и NDP в сетях на основе IPv6).

Адреса вроде MAC-48 наиболее распространены; они используются в таких технологиях, как Ethernet, Token ring, FDDI, WiMAX и др. Они состоят из 48 бит, таким образом, адресное пространство MAC-48 насчитывает 2^{48} (или 281 474 976 710 656) адресов. Согласно подсчётам IEEE, этого запаса адресов хватит по меньшей мере до 2100 года.

EUI-48 от MAC-48 отличается лишь семантически: в то время как MAC-48 используется для сетевого оборудования, EUI-48 применяется для других типов аппаратного и программного обеспечения.

Идентификаторы EUI-64 состоят из 64 бит и используются в FireWire, а также в IPv6 в качестве младших 64 бит сетевого адреса узла.

Ethernet

Ethernet - это самый распространенный на сегодняшний день стандарт локальных сетей. Общее количество сетей, использующих в настоящее время Ethernet, оценивается в 5 миллионов, а количество компьютеров, работающих с установленными сетевыми адаптерами Ethernet - в 50 миллионов.

Когда говорят Ethernet, то под этим обычно понимают любой из вариантов этой технологии. В более узком смысле, Ethernet - это сетевой стандарт, основанный на технологиях экспериментальной сети Ethernet Network, которую фирма Xerox разработала и реализовала в 1975 году (еще до появления персонального компьютера). Метод доступа был опробован еще раньше: во второй половине 60-х годов в радиосети Гавайского университета использовались различные варианты случайного доступа к общей радиосреде, получившие общее название Aloha. В 1980 году фирмы DEC, Intel и Xerox совместно разработали и опубликовали стандарт Ethernet версии II для сети, построенной на основе коаксиального кабеля. Поэтому стандарт Ethernet иногда называют стандартом DIX по заглавным буквам названий фирм

На основе стандарта Ethernet DIX был разработан стандарт IEEE 802.3, который во многом совпадает со своим предшественником, но некоторые различия все же имеются. В то время, как в стандарте IEEE 802.3 различаются уровни MAC и LLC, в оригинальном Ethernet оба эти уровня объединены в единый канальный уровень. В Ethernet определяется протокол тестирования конфигурации (Ethernet Configuration Test Protocol), который отсутствует в IEEE 802.3. Несколько отличается и формат кадра, хотя минимальные и максимальные размеры кадров в этих стандартах совпадают.

В зависимости от типа физической среды стандарт IEEE 802.3 имеет различные модификации - 10Base-5, 10Base-2, 10Base-T, 10Base-F.

Для передачи двоичной информации по кабелю для всех вариантов физического уровня технологии Ethernet используется манчестерский код.

Все виды стандартов Ethernet используют один и тот же метод разделения

среды передачи данных - метод CSMA/CD.

Теперь мы подробно рассмотрим применяемые стандарты Ethernet. Названия стандартов Ethernet расшифровываются следующим образом. Первый элемент — скорость передачи данных в Мбит/с. Второй элемент: Base — немодулированная передача, Broad — использование широкополосного кабеля с частотным уплотнением каналов. В третьем элементе число означает максимальную длину кабеля (хотя здесь есть противоречие со стандартом 1Base5, там длина кабеля — 250 м), а буква — одно из следующих сокращений: T — две витые пары, T4 — 4 витые пары, F — оптоволокно.

Например, 10Base-T означает, что данные передаются по двум витым парам при помощи немодулированной передачи со скоростью до 10 Мбит/с.

Ethernet ([ˈiːθər_net] от англ. *ether* [ˈiːθər] «эфир») — пакетная технология передачи данных преимущественно локальных компьютерных сетей.

Стандарты Ethernet определяют проводные соединения и электрические сигналы на физическом уровне, формат кадров и протоколы управления доступом к среде — на канальном уровне модели OSI. Ethernet в основном описывается стандартами IEEE группы 802.3. Ethernet стал самой распространённой технологией ЛВС в середине 1990-х годов, вытеснив такие устаревшие технологии, как Arcnet и Token ring.

История

Технология Ethernet была разработана вместе со многими первыми проектами корпорации Xerox PARC. Общепринято считать, что Ethernet был изобретён 22 мая 1973 года, когда Роберт Меткалф (*Robert Metcalfe*) составил докладную записку для главы PARC о потенциале технологии Ethernet. Но законное право на технологию Меткалф получил через несколько лет. В 1976 году он и его ассистент Дэвид Боггс (*David Boggs*) издали брошюру под названием «Ethernet: Distributed Packet-Switching For Local Computer Networks»^[1].

Меткалф ушёл из Xerox в 1979 году и основал компанию 3Com для продвижения компьютеров и локальных вычислительных сетей (ЛВС). Ему удалось убедить DEC, Intel и Xerox работать совместно и разработать стандарт

Ethernet (DIX). Впервые этот стандарт был опубликован 30 сентября 1980 года. Он начал соперничество с двумя крупными запатентованными технологиями: token ring и ARCNET, — которые вскоре были раздавлены под накатывающимися волнами продукции Ethernet. В процессе борьбы 3Com стала основной компанией в этой отрасли.

Технология

В стандарте первых версий (Ethernet v1.0 и Ethernet v2.0) указано, что в качестве передающей среды используется коаксиальный кабель, в дальнейшем появилась возможность использовать витую пару и оптический кабель.

Преимущества использования витой пары по сравнению с коаксиальным кабелем:

- возможность работы в дуплексном режиме;
- низкая стоимость кабеля «витой пары»;
- более высокая надёжность сетей при неисправности в кабеле (соединение точка-точка: обрыв кабеля лишает связи два узла. В коаксиале используется топология «шина», обрыв кабеля лишает связи весь сегмент);
- минимально допустимый радиус изгиба меньше;
- большая помехозащищённость из-за использования дифференциального сигнала;
- возможность питания по кабелю маломощных узлов, например IP-телефонов (стандарт Power over Ethernet, POE);
- гальваническая развязка трансформаторного типа. При использовании коаксиального кабеля в российских условиях, где, как правило, отсутствует заземление компьютеров, применение коаксиального кабеля часто сопровождалось пробоем сетевых карт и иногда даже полным «выгоранием» системного блока. [источник не указан 835 дней]

Причиной перехода на оптический кабель была необходимость увеличить длину сегмента без повторителей.

Метод управления доступом (для сети на коаксиальном кабеле) — множественный доступ с контролем несущей и обнаружением коллизий

(CSMA/CD, Carrier Sense Multiple Access with Collision Detection), скорость передачи данных 10 Мбит/с, размер пакета от 72 до 1526 байт, описаны методы кодирования данных. Режим работы полудуплексный, то есть узел не может одновременно передавать и принимать информацию. Количество узлов в одном разделяемом сегменте сети ограничено предельным значением в 1024 рабочих станции (спецификации физического уровня могут устанавливать более жёсткие ограничения, например, к сегменту тонкого коаксиала может подключаться не более 30 рабочих станций, а к сегменту толстого коаксиала — не более 100). Однако сеть, построенная на одном разделяемом сегменте, становится неэффективной задолго до достижения предельного значения количества узлов, в основном по причине полудуплексного режима работы.

В 1995 году принят стандарт IEEE 802.3u Fast Ethernet со скоростью 100 Мбит/с и появилась возможность работы в режиме полный дуплекс. В 1997 году был принят стандарт IEEE 802.3z Gigabit Ethernet со скоростью 1000 Мбит/с для передачи по оптическому волокну и ещё через два года для передачи по витой паре.

Формат кадра

Существует несколько форматов Ethernet-кадра.

- Первоначальный Version I (больше не применяется).
- Ethernet Version 2 или Ethernet-кадр II, ещё называемый DIX (аббревиатура первых букв фирм-разработчиков DEC, Intel, Xerox) — наиболее распространена и используется по сей день. Часто используется непосредственно протоколом Интернет.
 - Novell — внутренняя модификация IEEE 802.3 без LLC (Logical Link Control).
 - Кадр IEEE 802.2 LLC.
 - Кадр IEEE 802.2 LLC/SNAP.
 - Некоторые сетевые карты Ethernet, производимые компанией Hewlett-Packard использовали при работе кадр формата IEEE 802.12, соответствующий стандарту 100VG-AnyLAN.

В качестве дополнения Ethernet-кадр может содержать тег IEEE 802.1Q для идентификации VLAN, к которой он адресован, и IEEE 802.1p для указания приоритетности.

Разные типы кадра имеют различный формат и значение MTU.

MAC-адреса

При проектировании стандарта Ethernet было предусмотрено, что каждая сетевая карта (равно как и встроенный сетевой интерфейс) должна иметь уникальный шестибайтный номер (MAC-адрес), прошитый в ней при изготовлении. Этот номер используется для идентификации отправителя и получателя кадра, и предполагается, что при появлении в сети нового компьютера (или другого устройства, способного работать в сети) сетевому администратору не придётся настраивать MAC-адрес.

Уникальность MAC-адресов достигается тем, что каждый производитель получает в координирующем комитете IEEE Registration Authority диапазон из шестнадцати миллионов (2^{24}) адресов, и по мере исчерпания выделенных адресов может запросить новый диапазон. Поэтому по трём старшим байтам MAC-адреса можно определить производителя. Существуют таблицы, позволяющие определить производителя по MAC-адресу; в частности, они включены в программы типа arpalert.

Мак адрес считывается один раз из ПЗУ при инициализации сетевой карты, в дальнейшем все пакеты генерируются операционной системой. Все современные операционные системы позволяют поменять его. Для Windows начиная как минимум с Windows 98 он менялся в реестре. Некоторые драйвера сетевых карт давали возможность изменить его в настройках, но смена работает абсолютно для любых карт.

Некоторое время назад, когда драйверы сетевых карт не давали возможность изменить свой MAC-адрес, а альтернативные возможности не были слишком известны, некоторые провайдеры Internet использовали его для идентификации машины в сети при учёте трафика. Программы из Microsoft Office, начиная с версии Office 97, записывали MAC-адрес сетевой платы в

редактируемый документ в качестве составляющей уникального GUID-идентификатора.^[21] MAC адрес роутера передавался Mail.Ru агентом на свой сервер открытым текстом при логине.

Разновидности Ethernet

В зависимости от скорости передачи данных, и передающей среды существует несколько вариантов технологии. Независимо от способа передачи стек сетевого протокола и программы работают одинаково практически во всех нижеперечисленных вариантах.

В этом разделе дано краткое описание всех официально существующих разновидностей. По некоторым причинам, в дополнение к основному стандарту многие производители рекомендуют пользоваться другими запатентованными носителями — например, для увеличения расстояния между точками сети используется волоконно-оптический кабель.

Большинство Ethernet-карт и других устройств имеет поддержку нескольких скоростей передачи данных, используя автоопределение (autonegotiation) скорости и дуплексности, для достижения наилучшего соединения между двумя устройствами. Если автоопределение не срабатывает, скорость подстраивается под партнёра, и включается режим полудуплексной передачи. Например, наличие в устройстве порта Ethernet 10/100 говорит о том, что через него можно работать по технологиям 10BASE-T и 100BASE-TX, а порт Ethernet 10/100/1000 — поддерживает стандарты 10BASE-T, 100BASE-TX и 1000BASE-T.

Token Ring

Token Ring — технология локальной вычислительной сети (LAN) кольца с «маркёрным доступом» — протокол локальной сети, который находится на канальном уровне (DLL) модели OSI. Он использует специальный трёхбайтовый фрейм, названный маркёром, который перемещается вокруг кольца. Владение маркёром предоставляет право обладателю передавать информацию на носителе.

Кадры кольцевой сети с маркёрным доступом перемещаются в цикле.

Описание

Станции на локальной вычислительной сети (LAN) Token Ring логически организованы в звездообразную топологию с данными, передаваемыми последовательно от одной кольцевой станции до другой с управляющим маркером, циркулирующим вокруг кольцевого доступа управления. Этот механизм передачи маркёра совместно использован ARCNET, маркёрной шиной, и FDDI, и имеет теоретические преимущества перед стохастическим CSMA/CD Ethernet.

Передача маркёра

Token Ring и IEEE 802.5 являются главными примерами сетей с передачей маркёра. Сети с передачей маркёра перемещают по сети небольшой блок данных, называемый маркёром. Владение этим маркёром гарантирует право передачи. Если узел, принимающий маркёр, не имеет информации для отправки, он просто переправляет маркёр к следующей конечной станции. Каждая станция может удерживать маркёр в течение определенного максимального времени (по умолчанию — 10 мс).

Данная технология предлагает вариант решения проблемы коллизий, которая возникает при работе локальной сети. В технологии Ethernet, такие коллизии возникают при одновременной передаче информации несколькими рабочими станциями, находящимися в пределах одного сегмента, то есть использующих общий физический канал данных.

Если у станции, владеющей маркёром, имеется информация для передачи, она захватывает маркёр, изменяет у него один бит (в результате чего маркёр превращается в последовательность «начало блока данных»), дополняет информацией, которую он хочет передать и отсылает эту информацию к следующей станции кольцевой сети. Когда информационный блок циркулирует по кольцу, маркёр в сети отсутствует (если только кольцо не обеспечивает «раннего освобождения маркёра» — early token release), поэтому другие станции, желающие передать информацию, вынуждены ожидать. Следовательно, в сетях

Token Ring не может быть коллизий. Если обеспечивается раннее высвобождение маркера, то новый маркер может быть выпущен после завершения передачи блока данных.

Информационный блок циркулирует по кольцу, пока не достигнет предполагаемой станции назначения, которая копирует информацию для дальнейшей обработки. Информационный блок продолжает циркулировать по кольцу; он окончательно удаляется после достижения станции, отославшей этот блок. Станция отправки может проверить вернувшийся блок, чтобы убедиться, что он был просмотрен и затем скопирован станцией назначения.

Сфера применения

В отличие от сетей CSMA/CD (например, Ethernet) сети с передачей маркера являются детерминистическими сетями. Это означает, что можно вычислить максимальное время, которое пройдет, прежде чем любая конечная станция сможет передать. Эта характеристика, а также некоторые характеристики надежности, делают сеть Token Ring идеальной для применений, где задержка должна быть предсказуема и важна устойчивость функционирования сети. Примерами таких применений является среда автоматизированных станций на заводах.

Применяется как более дешёвая технология, получила распространение везде, где есть ответственные приложения, для которых важна не столько скорость, сколько надёжная доставка информации. В настоящее время Ethernet по надёжности не уступает Token Ring и существенно выше по производительности.

История

Изначально технология была разработана компанией IBM в 1984 году. В 1985 году комитет IEEE 802 на основе этой технологии принял стандарт IEEE 802.5. В последнее время даже в продукции IBM доминируют технологии семейства Ethernet, несмотря на то, что ранее в течение долгого времени компания использовала Token Ring в качестве основной технологии для построения локальных сетей^[1].

В основном, технологии похожи, но имеются незначительные различия.

Token Ring от IBM описывает топологию «звезда», когда все компьютеры присоединены к одному центральному устройству (англ. *multistation access unit (MSAU)*), в то время, как IEEE 802.5 не заостряет внимания на топологии.

Модификации Token Ring

Существуют 2 модификации по скоростям передачи: 4 Мбит/с и 16 Мбит/с. В Token Ring 16 Мбит/с используется технология раннего освобождения маркера. Суть этой технологии заключается в том, что станция, «захватившая» маркёр, по окончании передачи данных генерирует свободный маркёр и запускает его в сеть. Попытки внедрить 100 Мбит/с технологию не увенчались коммерческим успехом. В настоящее время технология Token Ring считается устаревшей.

FDDI

FDDI (англ. *Fiber Distributed Data Interface* — Волоконно-оптический интерфейс передачи данных) — стандарт передачи данных в локальной сети, протянутой на расстоянии до 200 километров. Стандарт основан на протоколе Token Ring. Кроме большой территории, сеть FDDI способна поддерживать несколько тысяч пользователей.

В качестве среды передачи данных в FDDI рекомендуется использовать волоконно-оптический кабель, однако можно использовать и медный кабель, в таком случае используется сокращение CDDI (Copper Distributed Data Interface). В качестве топологии используется схема двойного кольца, при этом данные в кольцах циркулируют в разных направлениях. Одно кольцо считается основным, по нему передаётся информация в обычном состоянии; второе — вспомогательным, по нему данные передаются в случае обрыва на первом кольце. Для контроля за состоянием кольца используется сетевой маркер, как и в технологии Token Ring.

Поскольку такое дублирование повышает надёжность системы, данный стандарт с успехом применяется в магистральных каналах связи.

История

Стандарт был разработан в середине 80-х годов Национальным Американским Институтом Стандартов (ANSI) и получил номер ANSI X3T9.5.

Оптическое волокно — нить из оптически прозрачного материала (стекло, пластик), используемая для переноса света внутри себя посредством полного внутреннего отражения.

Волоконная оптика — раздел прикладной науки и машиностроения, описывающий такие волокна. Кабели на базе оптических волокон используются в волоконно-оптической связи, позволяющей передавать информацию на большие расстояния с более высокой скоростью передачи данных, чем в электронных средствах связи. В ряде случаев они также используются при создании датчиков.

2.1. Компоненты компьютерных сетей и топологии их взаимодействия

2.1.1. Компоненты локальных компьютерных сетей

Локальные сети стали неотъемлемым атрибутом современной рабочей среды. Топологию и архитектуру локальных сетей намного проще понять после их разбиения на физические компоненты. Часто архитектура сети разделяется на уровни с уникальными наборами функциональных возможностей в соответствии с эталонной моделью (ЭМ) взаимодействия открытых систем (ВОС, OSI).

Необходимыми условиями такого разложения архитектуры локальной сети на уровни является объяснение двух ее свойств: топологии взаимодействия и методологии доступа к ресурсам. Методология доступа к ресурсам локальной сети описывает способ совместного использования ресурсов: компонент подключенных к сети. Часто эта характеристика сети называется ее типом. С точки зрения типа наиболее распространенными являются архитектуры одноранговых сетей и сети с топологией клиент/сервер.

Топология локальной сети описывает физическое расположение концентраторов и кабелей. Основными топологиями считаются шинная, кольцевая, звездообразная и коммутируемая.

Вместе перечисленные свойства помогают подготовить почву для подробного исследования функциональных уровней архитектуры локальной сети. В главе описаны основные комбинации типов архитектур и топологий локальных сетей, а также их преимущества, ограничения и возможные области применения.

Для рассмотрения и анализа типов локальных сетей и их топологий необходимо вначале познакомиться с некоторыми из основных компонент локальной сети. Наиболее распространенными из них являются автоматизированные рабочие места (АРМ, точнее компьютеры) пользователей (клиентов) и серверы. К основным компонентам относятся те устройства, которые непосредственно обращаются к другим устройствам или к которым могут

обратиться другие устройства.

Сервер - это любой компьютер, подключенный к локальной сети, на котором находятся ресурсы, используемые другими устройствами локальной сети. Рабочее место - это любой компьютер, который через локальную сеть обращается к ресурсам, хранящимся на серверах приложений, файловом (СП, СФ) и принт-сервер (ПС).

Часто среди основных ресурсов выделяют принтеры. Принтеры - это, естественно, устройства вывода, которые создают жесткие копии файлов. Через локальную сеть можно также обращаться к множеству других устройств, таких как накопители CD-ROM, но эти устройства относятся к вспомогательным, подключаемым к основным. Такое подключение одних устройств к другим, например, накопителя CD-ROM к серверу, называется подчинением. Принтеры могут либо подчиняться основным устройствам, либо сами являться основными устройствами, подключенными непосредственно к сети.

Слово "сервер" часто используется для обобщенного описания всех многопользовательских компьютеров. Однако следует заметить, что серверы могут выполнять совершенно различные задачи. Они обычно специализируются по своим функциям и описываются дополнительным образом (например, файл-сервер, сервер печати или сервер приложений).

Файл-серверы.

Одним из наиболее распространенных и знакомых широкому кругу пользователей является специализированный файл-сервер, который предоставляет возможность централизованного хранения файлов, используемых группой пользователей. Централизованное расположение файлов обладает рядом преимуществ по сравнению с распределением файлов по многим клиентским компьютерам. Вот некоторые из этих преимуществ:

1. Централизованное размещение. Все пользователи обращаются к одному постоянному хранилищу файлов общего пользования. Это предоставляет

двойную выгоду - пользователи освобождаются от необходимости ведения поиска файлов на нескольких компьютерах; все файлы находятся в одном месте. Пользователи также освобождаются от выполнения процедуры подключения к каждому компьютеру. Единожды войдя в сеть, они получают доступ ко всем необходимым файлам.

2. Защита от сбоев электропитания - использование одного централизованного сервера для хранения файлов позволяет использовать различные методы защиты данных от сбоев электропитания. Колебание частоты напряжения или внезапное отключение питания может повредить как данные, так и аппаратное обеспечение компьютера. Источник бесперебойного питания, компенсирующий скачки напряжения и предоставляющий в случае отключения внешнего питания возможность питания от резервных аккумуляторных батарей, выгодно установить только на отдельном сервере. Аналогичная защита в одноранговых сетях потребовала бы более высоких затрат, поскольку потребовалось бы защищать большее количество компьютеров.

3. Удобное архивирование данных - хранение всех файлов совместного пользования на специально выделенном для этого сервере существенно упрощает их резервирование, так как в результате представляется возможность использовать единственное устройство вывода. Децентрализованное хранение данных означает, что данные с каждой рабочей станции должны резервироваться отдельно. Резервирование является основной мерой защиты данных от потери или повреждения. Подходящими устройствами для резервирования являются пишущие оптические накопители и даже жесткие диски. В соответствии с технологией параллельной записи для резервирования может одновременно использоваться несколько жестких дисков. Хотя эта технология в основном применяется для повышения скорости чтения данных, она также может использоваться для дублирования каждой операции записи.

Базовый сервер является более устойчивой и корректно настроенной платформой, чем типичное автоматизированное рабочее место (АРМ) в виде клиентского компьютера. Это обуславливает заметное повышение

производительности в операциях извлечения файлов по сравнению с одноранговыми сетями.

Использование файл сервера не всегда приводит к повышению производительности К локальным файлам всегда можно обратиться быстрее, чем к файлам, хранящимся на удаленном компьютере и передаваемым через локальную сеть Здесь имеется в виду повышение производительности по сравнению с извлечением файлов с других компьютеров одноранговой сети, а не по сравнению с чтением файлов с локального жесткого диска.

Далеко не все файлы подходят для хранения на файл-сервере Секретные, конфиденциальные файлы или файлы, предназначенные для ограниченного числа пользователей, лучше оставить на локальном жестком диске Хранение таких файлов на файл-сервере, естественно, предоставит все соответствующие преимущества (например, возможность автоматизированного резервирования), но одновременно повысит риск их разглашения.

Серверы приложений.

Серверы также часто используются в качестве централизованного хранилища прикладного программного обеспечения Серверы приложений, которые при поверхностном рассмотрении похожи на файл-серверы, являются в своем роде особыми. На сервере приложений хранится исполняемое прикладное программное обеспечение. Чтобы запустить такое приложение, клиент должен установить соединение с сервером через сеть. Приложение выполняется на этом сервере, а не на клиентском компьютере. Серверы, которые позволяют клиентам загружать копии приложения для выполнения на своем компьютере, являются файл-серверами. Просто в этом случае файлами являются исполняемые файлы приложений, но сервер все равно функционирует как файл сервер.

Серверы приложений позволяют организации сократить общие расходы на прикладное программное обеспечение. Приобретение и обслуживание одной многопользовательской копии приложения обычно обходится намного дешевле,

чем приобретение и обслуживание отдельных копий для каждого клиентского компьютера.

Серверы печати.

Серверы также предоставляют возможность совместного использования принтеров пользователями локальной сети. Хотя стоимость принтеров, особенно лазерных, существенно снизилась со времени их появления, многие организации еще не могут позволить себе поставить по принтеру на каждый рабочий стол. Вместо этого для совместного использования одного или нескольких принтеров всеми пользователями организуются серверы печати. Единственная функция сервера печати сводится к приему запросов на печать от всех сетевых устройств, помещению их в очередь на соответствующий принтер. Соответствующая архитектура проиллюстрирована на рисунке 2.1.



АРМ – автоматизированное рабочее место

СП – сервер приложений

ФС – файловый сервер

СПе – сервер печати

Рис 2.1 Функциональная структура компьютерных компонент локальной сети

Каждый принтер, подключенный к серверу печати, обладает собственной очередью или списком ожиданий. В этой очереди сохраняется порядок всех запросов, которые временно хранятся на сервере и ожидают вывода на принтер.

Запросы обычно обрабатываются в том порядке, в котором они были приняты. Клиентские операционные системы Microsoft Windows 95 и Windows NT Workstation допускают совместное использование принтеров.

Альтернативой организации сервера печати является непосредственное подключение принтера к локальной сети. Многие принтеры обладают сетевым адаптером, позволяющим напрямую подключить их к локальной сети, превращая в сервер очередей печати. Подключение принтеров непосредственно к локальной сети оправданно во всех случаях (исключение составляют сети, пользователи которых только и делают, что постоянно печатают).

На рисунке 2.1. показаны основные компоненты локальной сети, а также взаимосвязь вспомогательных и основных ресурсов сети.

Инсталляция коммерческой однопользовательской версии приложения на сервере приложений или файл-сервере может нарушить условия соглашения об авторских правах. Точно так же, как отдельный пользователь может передать кому-то оригинальный дистрибутив для инсталляции приложения, сервер может сделать копию программы доступной всем пользователям сети. Это является пиратством программного обеспечения, о чем должен знать каждый студент! Перед инсталляцией любого приложения на сервере убедитесь в том, что при его приобретении заключена какая-либо форма многопользовательского соглашения.

Хотя обычно желательно разделять прикладное программное обеспечение от файлов данных, используя для этого разные серверы (например, сервер приложений и файл-сервер), из этого правила есть одно важное исключение. Дело в том, что некоторые приложения создают и обслуживают большие реляционные базы данных. Эти приложения и их базы данных должны быть расположены на одном и том же сервере приложений.

Причина этого проста: механизм получения данных из базы данных принципиально отличается от простого извлечения файла Word или Excel. Приложение реляционной базы данных выталкивает только запрашиваемые данные и хранит все остальное в своей базе данных. Приложения автоматизации офисных операций, такие как Word и Excel, хранят информацию в автономных

файлах, которые обычно не содержат сложной структуры взаимозависимостей с другими данными. Приложение реляционной базы данных непосредственно отвечает за целостность базы данных и ее индексов. Управление базой данных через сеть увеличивает риск повреждения индексов и вывода приложения из строя.

2.1.2. Одноранговая архитектура функциональной структуры локальных сетей

Топология и количество компонент сети обуславливаются типом ее архитектуры. Тип архитектуры сети описывает способ доступа к подключенным ресурсам. В качестве ресурсов могут выступать компьютеры клиентов, серверы или любые устройства, файлы и т.д., принадлежащие клиенту или серверу. К этим ресурсам можно обращаться одним из двух способов: через одноранговые сети или через сети поддерживающие технологию клиент/сервер. И те и другие могут иметь как кабельные соединения (проводная связь), так и беспроводные соединения (мобильная связь).

Одноранговая сеть (peer-to-peer network) предоставляет неструктурированный доступ к сетевым ресурсам. Каждое устройство в одноранговой сети может быть и рабочим местом (компьютером клиента), и сервером одновременно. Все устройства могут напрямую обращаться к данным, программному обеспечению и другим сетевым ресурсам. Другими словами, каждый сетевой компьютер имеет равные права (находится в одном ранге) со всеми остальными сетевыми компьютерами - какая-либо иерархия в данном случае отсутствует (рис. 2.2).



Рис. 2.2. Функциональная структура одноранговой архитектуре сети.

Преимущества (одноранговой архитектуры)

Четыре основных преимущества одноранговой архитектуры:

- Одноранговые сети относительно легко развернуть. Тем не менее, такая сеть представляет собой немного больше, чем множество клиентских компьютеров с сетевой операционной системой, допускающей одноранговое совместное использование ресурсов. Таким образом, развертывание одноранговой сети требует только приобретения и инсталляции концентратора или концентраторов, компьютеров, кабелей и операционной системы, которая поддерживает такой доступ к ресурсам.

- Одноранговые сети, кроме того, недорогие в эксплуатации. В них отсутствуют дорогостоящие и сложные выделенные серверы, которые требуют специального администрирования и создание особых климатических условий. Отсутствие выделенных серверов также снижает расходы на их обслуживание и обучение персонала, а также дополнительные расходы на создание специально для серверов комнаты с управляемым климатом. Каждый компьютер расположен, по крайней мере теоретически, на рабочем месте и обслуживается его основным пользователем.

- Одноранговые сети можно разворачивать с помощью таких известных операционных систем, как Windows 95, Windows NT и Windows for Workgroups.

- Отсутствие иерархической зависимости делает одноранговую сеть более отказоустойчивой, чем сеть на основе сервера. Теоретически в сети архитектуры клиент/сервер самым уязвимым компонентом является сервер. Это означает, что сбой на сервере может повлиять на работоспособность всей сети. В одноранговой сети сбой любого компьютера приводит к недоступности лишь некоторого подмножества сетевых ресурсов.

Недостатки (одноранговой архитектуры)

Одноранговая архитектура сети не лишена недостатков. Наиболее

серьезные ограничения касаются области безопасности, производительности и администрирования.

Для одноранговой сети характерны следующие недостатки, связанные с безопасностью:

- Пользователи вынуждены запоминать множество паролей, обычно по одному для каждого компьютера, к которому необходим доступ.

- Отсутствие централизованного хранилища ресурсов общего пользования усложняет поиск необходимой информации. Эту проблему можно решить, заставив всех членов рабочей группы соблюдать определенные соглашения и процедуры. Пользователи имеют привычку придумывать очень "творческие" способы копирования с избытком паролей. Большинство из этих способов ставит под угрозу безопасность каждого компьютера в одноранговой сети.

Как и устройства, подключенные к сети, безопасность равномерно распределяется по всей одноранговой сети. Меры безопасности в такой сети обычно сводятся к аутентификации пользователей с помощью идентификаторов и паролей, а также к выделению определенных прав доступа к конкретным ресурсам. "Администратор" каждого сетевого компьютера самостоятельно назначает эти права для всех остальных пользователей сети.

Хотя каждого пользователя одноранговой сети можно считать администратором своего компьютера, рядовые пользователи редко обладают знаниями и умениями, необходимыми для профессионального выполнения административных задач. Зачастую даже в отдельных рабочих группах нет ни одного квалифицированного администратора. Это один из недостатков одноранговых сетей.

К сожалению, обычно не все пользователи обладают одинаковой (и достаточной) технической квалификацией. Следовательно, безопасность всей сети зависит от умений и способностей ее наименее технически образованного члена! Эту ситуацию можно сравнить с метафорой цепи. Цепь настолько прочна, насколько прочно ее самое слабое звено. Безопасность в одноранговой сети настолько сильна, насколько силен ее самый слабый компонент.

Хотя необходимость администрирования в одноранговой сети меньше, чем в сети клиент/сервер, это администрирование распределяется между всеми пользователями. В результате возникает несколько логических вопросов. Два наиболее актуальных из них:

- Некоординированное и, возможно, нерегулярное резервирование данных и программного обеспечения. Каждый пользователь отвечает только за свой собственный компьютер и в большинстве случаев выполняет резервирование только тогда, когда у него появляется свободное время.

- Отсутствие ответственности за соблюдение соглашений об именовании и расположении файлов. Учитывая отсутствие центрального хранилища информации и какой-либо логики в организации ресурсов локальной сети, становится довольно сложно отследить расположение определенной информации. Как и все остальные аспекты одноранговой сети, эффективность в целом напрямую зависит от методов и процедур, которых придерживаются все участники.

И, наконец, производительность также страдает. В одноранговой сети каждый компьютер является многопользовательским. Типичный компьютер лучше справляется с задачами однопользовательского клиента, чем с многопользовательской поддержкой. Следовательно, производительность любого компьютера заметно снижается (с точки зрения его основного пользователя) в тот момент, когда какой-либо удаленный пользователь подключается к нему и начинает использовать его ресурсы.

Файлы и другие ресурсы компьютера одноранговой сети настолько доступны, насколько доступен сам этот компьютер. Другими словами, если основной пользователь компьютера вышел из офиса и выключил свой компьютер, его ресурсы становятся недоступными для остальных компьютеров сети. Такую ситуацию можно обойти, если постоянно оставлять включенными все компьютеры, но тогда страдает безопасность.

Еще одним, более тонким аспектом производительности является возможность расширения. Одноранговая методология по своей сути не

расширяемая. Чем больше компьютеров одновременно работает в одноранговой сети, тем более неуправляемой становится эта сеть.

Особенности одноранговых беспроводных сетей

Одноранговые сети имеют два основных применения. Во-первых, они идеально подходят для маленьких организаций с ограниченным бюджетом и ограниченными потребностями в совместном использовании информации. Кроме того, рабочие группы внутри больших организаций также могут использовать эту методологию для более тесного сотрудничества внутри группы.

Технологии построения одноранговых беспроводных локальных сетей (БЛВС - WLAN, wireless local area network), составляют быстро развивающийся рынок. БЛВС позволяют использовать гибкий беспроводный доступ. В отличие от технологий, описанных выше, радиус охвата БЛВС ограничен размерами отдельной комнаты, здания, студенческого городка и т. п., а предоставляются эти сети отдельными, не глобальными сетевыми поставщиками. Основной целью беспроводных локальных сетей является замена существующих кабельных локальных сетей с, дополнительным, введением высокой гибкости обеспечивая мобильную связь. Ниже перечислены основные достоинства и недостатки беспроводных локальных сетей по сравнению с их проводными аналогами.

Достоинства беспроводных локальных сетей:

- Гибкость. Радиоволновая физическая природа БЛВС обеспечивает большую степень свободы пользователей сети. Для радиосетей нет ограничений, характерных для кабельных сетей. Радиоволны беспрепятственно проникают сквозь видимые преграды, приемники и передатчики могут располагаться где угодно, например, скрыты в стенах и т.д. Для кабельных сетей требования пожарной безопасности в зданиях и помещениях ограничивают возможности быстрого проектирования и разворачивания сети.

- Планирование. Поддерживая в своих устройствах режим мобильной связи, можно построить разветвленные сети с самой различной топологией

соединений. Для проводных сетей в первую очередь необходимо проектирование кабельной инфраструктуры; возможны проблемы с правильным подключением, иногда требуется установка коммутаторов.

Слабые стороны беспроводных локальных сетей:

- Слабая помехозащищенность приводит к увеличению частоты появления ошибок при передаче (10^{-6} по сравнению с 10^{-10} для оптоволоконных сетей), большим задержкам/увеличению дисперсии задержек.

- Регулирование в области беспроводных технологий связи производится на государственные органы. В мире существуют правительственные и неправительственные институты, занимающиеся стандартами, ограничивающими и регулирующими деятельность в области радиосвязи, распределением частотного диапазона для уменьшения интерференции. В рамках национальных программ процессы становления занимают длительное время. Поэтому беспроводные локальные сети ограничиваются маломощными передатчиками, и для них выделяется нелицензируемый диапазон частот.

- Безопасность и защита. Передача данных с использованием радиочастот подвержена помехам со стороны технологичных приборов и устройств. Поэтому должны быть предусмотрены соответствующие меры предосторожности. Кроме того, открытый радиointерфейс делает возможным несанкционированный доступ к данным, тогда как «прослушивание» оптоволоконных сетей сложнее. Разные и порой противоречивые идеи были заложены в основу беспроводных локальных сетей с целью обеспечения их коммерческого успеха.

- Энергосбережение: Устройства, связывающиеся через беспроводные локальные сети, - это обычно мобильные беспроводные аппараты, питающиеся от батарей. С учетом этого разработчики локальных сетей проектируют энергосберегающие варианты, модели с функциями управления энергопотреблением. Устройства беспроводной связи лишь в некоторых случаях используют стационарное сетевое питание от электророзеток, когда нет необходимости заново проводить электропитание в зданиях. Однако, будущее принадлежит носимым устройствам без ограничивающих проводов.

- Помехоустойчивые технологии связи. По сравнению со своими проводными аналогами беспроводные локальные сети эксплуатируются в более сложных условиях. Так как сети используют радиосвязь, возможны помехи, наводимые другими электрическими приборами. Кроме того, применяемые в БЛВС ненаправленные антенны не всегда обеспечивают надежную связь.

- Самоорганизующаяся сеть со случайными связями. Используется на практике, когда нужно быстро развернуть сеть, полагаясь на вероятную возможность связи между узлами. Такие БЛВС не требуют сложных процедур инициализации и запускаются сразу при включении, однако, они не обеспечат всех возможностей эпизодических сетей.

В настоящее время в БЛВС используются два основных способа передачи данных. Это технология с использованием инфракрасного излучения (например, с длиной волны 900 нм) и связь с помощью радиоволн в гигагерцевом диапазоне (например, нелицензируемый ISM диапазон 2,4 ГГц). Обе эти технологии поддерживают организацию мобильных сетей. Например, обеспечивают информационный обмен между настольным ПК и удаленным принтером, поддерживают мобильность пользователей сети небольшого радиуса действия.

Возможны два способа связи в инфракрасном диапазоне. В одном случае приемник и передатчик находятся в зоне прямой видимости и используют направленное излучение либо устанавливаются адаптеры так называемого диффузного типа, передатчики которых излучают сигналы в полусферической области. Такие ИК-лучи претерпевают многократное отражение от потолка, стен и прочих поверхностей, что позволяет переносить мобильные ПК в пределах помещения, не теряя контакта с ИК-устройством. В качестве излучателя ИК-лучей могут использоваться обычный светодиод либо лазерный диод. Приемником сигнала является фотодиод. Подробное описание технологии (принципы модуляции, факторы ухудшения качества) можно найти в работах [Wesel, 1998] и [Santamaria, 1994].

К основным преимуществам ИК-технологии относится низкая стоимость приемников и передатчиков инфракрасного излучения. Большинство

портативных ПК, ноутбуков, PDA, мобильных телефонов снабжены адаптерами ИК-лучей. Версия 1.0 промышленного стандарта ИК-технологии устанавливает максимальную скорость передачи данных в 115 Кбит/с. По версии 1.1 пропускная способность ИК-каналов увеличена до 1,152 Мбит/с и 4Мбит/с. Использование ИК-диапазона не лицензируется, передача данных в этом диапазоне мало подвержена помехам от электроприборов.

К недостаткам сетей ИК-диапазона относится небольшая пропускная способность каналов. Ограничение скорости передачи 4 Мбит/с существенно по сравнению с проводными локальными сетями. Причем наибольшая скорость и качество связи достигаются в зоне прямой видимости передатчика и приемника, любой предмет на пути ИК-лучей является препятствием для их прохождения.

Почти все БЛВС, рассматриваемые в настоящей книге, используют радиоволновый способ передачи данных. Аналогами в мобильной беспроводной телефонной связи в радиоволновом диапазоне являются стандарт GSM 900, 1 800 и 1900 МГц, а также стандарт DECT 1880 МГц.

К достоинствам радиопередачи относится большой опыт разработок в радиосвязи и передаче данных мобильных сотовых систем и территориально-распределенных сетей. Радиоволновый способ передачи имеет меньше ограничений при распространении сигнала и большую пропускную способность (10 Мбит/с) по сравнению с ИК-лучами.

В тоже время слабая помехозащищенность радиосигнала от электрических возмущений и межсетевых влияний, а также необходимость получения лицензии на использование радиочастот для своего оборудования являются недостатками использования радиоволнового диапазона.

Из трех технологий БЛВС в книге рассматривается только стандарт IEEE 802.11 сети Radio Ethernet и HIPERLAN наряду с радиопередачей описывает сети на основе ИК-лучей. Сеть HIPERLAN работает в радиоволновом диапазоне.

2.1.3. Многогранговая архитектура локальных сетей

В сетях обеспечивающих реализацию многогранговой архитектуры в технологии клиент/сервер отличием от одноранговых является то, что у нее за счет выделенных серверов появляется иерархия, призванная упростить управление различными функциями сети по мере увеличения ее размера. Часто подобные сети называются сетями архитектуры клиент/ сервер (рис.2.3).



Рис. 2.3. Двухранговая архитектура локальной сети как технология клиент/сервер.

В подобных сетях основная часть совместно используемых ресурсов сосредоточена на отдельных компьютерах, называемых серверами. На серверах обычно нет основных пользователей. Вместо этого они являются многопользовательскими компьютерами, предоставляющими возможность совместного использования своих ресурсов клиентам сети. В результате клиенты освобождаются от нагрузки, связанной с функционированием в качестве серверов для других клиентов.

Преимущества

Серверному подходу присуще множество преимуществ, связанных с доступом к сетевым ресурсам. Эти преимущества прямо соответствуют

ограничениям одноранговых сетей и затрагивают области безопасности, производительности и администрирования.

В сетях серверной архитектуры можно поддерживать более строгую безопасность, чем в одноранговых сетях. Этому способствует несколько факторов. Во-первых, безопасность контролируется централизованно. Сетевые ресурсы больше не зависят от теории "наиболее слабого звена", которая была свойственна одноранговой сети.

Вместо этого учетные записи всех пользователей (называемые также идентификаторами или бюджетами) и пароли централизованно управляются и сверяются перед тем, как пользователь получает доступ к запрашиваемому ресурсу. Такой подход одновременно упрощает жизнь пользователям, освобождая их от необходимости запоминать множество паролей.

Еще одним преимуществом централизации ресурсов является упрощение регулярного и надежного выполнения административных задач, таких как резервирование.

Сети клиент/сервер несколькими способами способствуют увеличению производительности сетевых компьютеров. Во-первых, каждый клиент освобождается от нагрузки, связанной с обработкой запросов от других клиентов. Каждый клиент в такой сети заботится только о выполнении запросов, сгенерированных его основным (и единственным!) пользователем. Что более важно, обработка запросов перепоручается серверу, конфигурация которого специально оптимизирована для выполнения соответствующих задач. Обычно на сервере устанавливаются более мощные процессоры, больше памяти и более объемные и быстрые дисковые накопители, чем на клиентских компьютерах. Это приводит к повышению производительности клиентских компьютеров и повышению оперативности выполнения запросов к ресурсам, централизованным на сервере.

Кроме того, пользователям не нужно запоминать, где располагаются определенные ресурсы, как это было в одноранговых сетях. В сетях архитектуры клиент/сервер количество возможных мест хранения ресурсов сокращено до

количества серверов в сети. В серверной среде Microsoft Windows NT на ресурсы сервера можно ссылаться как на логические диски. После подключения сетевого диска пользователь может так же легко обращаться к удаленным ресурсам, как к локальным ресурсам собственного компьютера.

Помимо этого сети серверной архитектуры очень легко расширяются. Независимо от количества клиентов, подключенных к сети, ресурсы всегда хранятся централизованно. Управление и контроль за безопасностью этих ресурсов также всегда осуществляются централизованно. Следовательно, производительность всей сети не страдает при увеличении ее размера.

Недостатки серверной архитектуры

Сеть на основе сервера имеет одно ограничение: ее развертывание и эксплуатация обходится намного дороже одноранговой сети. Эта существенная разница в стоимости состоит из множества аспектов.

Во-первых, расходы на аппаратное и программное обеспечение существенно увеличиваются из-за необходимости установки отдельного сетевого компьютера, обслуживающего клиентов. Серверы могут быть довольно изощренными и, следовательно, дорогими компьютерами.

Во-вторых, стоимость эксплуатации сети клиент/сервер также намного выше. Это связано с необходимостью приема на работу квалифицированного специалиста, администрирующего сеть и ее серверы. В одноранговой сети каждый пользователь сам отвечает за обслуживание своего компьютера; для выполнения этих функций можно не назначать отдельного человека.

В третьих, следует учитывать стоимость возможного простоя. В одноранговой сети выход из строя одного компьютера означает недоступность лишь небольшого количества ресурсов. В сети клиент/сервер выход из строя сервера может затронуть практически всех пользователей. Это увеличивает потенциальный риск для бизнеса при использовании сети с выделенными серверами. Для уменьшения этого риска используется множество подходов,

включая кластеризацию серверов с целью достижения приемлемого уровня избыточности. К сожалению, каждый из этих подходов еще больше увеличивает стоимость сети.

Область применения

Сети с серверами оказываются очень эффективны в больших организациях. Такие сети также могут быть полезными в любых обстоятельствах, требующих соблюдения более строгой безопасности или более четкого управления ресурсами. Однако небольшие организации не могут позволить себе развернуть сети архитектуры клиент/сервер из-за их высокой стоимости.

Отличие между одноранговой сетью и сетью с выделенными серверами не такое уж и четкое, как может показаться после прочтения предыдущих разделов. В учебных целях они преднамеренно были представлены как различные типы сетей. В действительности отличия между ними стираются благодаря возможностям многих операционных систем, таких как Microsoft Windows for Workgroups, Windows 95 и Windows NT.

Сегодня широко используются комбинации однорангового и серверного доступа к ресурсам одной сети. Примером может служить сеть с сервером, на котором централизованы ресурсы для универсального использования. Локальные рабочие группы такой сети могут предоставлять одноранговый доступ к своим ресурсам для своих внутренних нужд.

2.2. Топологии локальных сетей

Топологии локальных сетей можно описывать как с физической, так и с логической точки зрения. Физическая топология описывает геометрическое расположение компонентов локальной сети. Топология - это не карта сети. Это теоретическая конструкция, которая графически передает форму и структуру локальной сети.

Логическая топология описывает возможные соединения между парами конечных точек сети, которые в состоянии взаимодействовать. Эта информация оказывается полезной при описании наборов конечных точек, которые могут взаимодействовать друг с другом, и определении наличия прямых физических соединений (точнее каналов связи физического уровня ЭМ ВОС) между парами конечных точек. В этой главе внимание сосредоточено исключительно на физических топологиях.

До недавнего времени существовало три основные топологии: шинная, кольцевая и звездообразная. Каждая основная топология зависит от выбранной физической технологии локальной сети. Например, в сетях Token Ring по определению используются кольцевые топологии. Однако устройства MSAU (концентраторы Token Ring или модули многостанционного доступа - Multiple-Station Access Unit) стирают различие между кольцевой и звездообразной топологией для сетей Token Ring. В результате появляется звездно-кольцевая топология. Точно так же появление устройств коммутации в локальных сетях опять изменяет представление о топологиях. Коммутируемые локальные сети независимо от типа кадра и метода доступа похожи по топологии. Кольцо, существующее на физическом уровне в Token Ring, при использовании модулей MSAU оказывается больше не связанным со всеми устройствами, подключенными к концентратору. Вместо этого каждое устройство организует свое собственное мини-кольцо, в котором участвуют только два устройства: устройство станции и порт коммутатора. Следовательно, коммутируемую топологию теперь можно добавить в качестве четвертой к привычной тройке

основных топологий локальных сетей.

Коммутаторы реализуют звездообразную топологию независимо от того, для какого протокола канального уровня они спроектированы. Учитывая, что слово "коммутатор" легко воспринимается (благодаря непрекращающимся маркетинговым кампаниям изготовителей коммутаторов), понятие "коммутатора" стало более содержательным, чем "топология звезда-магистраль" или "топология звезда-кольцо". Следовательно, коммутацию можно считать самостоятельной топологией. Новая формулировка процессов коммутации расширила историческое объединение топологий и технологий локальных сетей - практически во всех топологиях может использоваться коммутирующее оборудование. Это оказывает существенное влияние на доступ к сети и, следовательно, на общую производительность сети.

2.2.1. Шинная топология

В шинной топологии все сетевые узлы равноправно соединены между собой с помощью одного открытого кабеля. Этот кабель может поддерживать только один канал и называется шиной. В некоторых шинных технологиях используется более одного кабеля. Следовательно, они в состоянии поддерживать более одного канала, хотя каждый кабель остается только одним каналом передачи.

Оба конца кабеля должны оканчиваться резистивной нагрузкой, называемой оконечным резистором. Эти резисторы предназначены для предотвращения отражения сигналов. Когда станция передает сигнал в кабель, этот сигнал распространяется в обоих направлениях. Если оконечный резистор не установлен, достигая конца шины сигнал меняет свое направление. В результате одна передача может полностью захватить всю полосу пропускания сети и препятствовать передаче от других станций.

Пример шинной топологии показан на рисунке 2.4. В типичной шинной

топологии используется единственный кабель, не требующий установки внешних электронных устройств и соединяющий все узлы сети как равноправные устройства. Все подключенные устройства прослушивают трафик шины и принимают только адресованные им пакеты. Благодаря отсутствию каких-либо внешних электронных устройств, таких как повторители, локальная сеть шинной топологии оказывается простой и недорогой. К ее недостаткам относятся серьезные ограничения на расстояние, функциональные возможности и расширяемость.

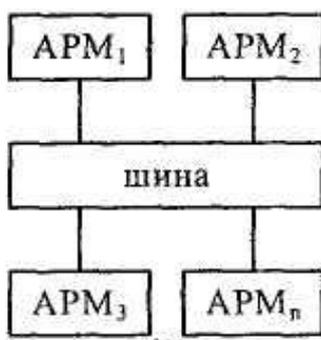


Рис. 2.4. Шинная топология.

Эту топологию целесообразно использовать лишь в небольших локальных сетях. Поэтому доступные сегодня коммерческие сетевые продукты, использующие шинную топологию, позволяют развернуть лишь недорогие одноранговые сети, предоставляющие только основные возможности взаимодействия. Такие сети предназначены для домашних и небольших офисов.

Единственным исключением являлась локальная сеть Token Bus, соответствующий стандарт спецификации IEEE 802.4. Эта технология была довольно надежной и детерминистической, во многом напоминая стандарт Token Ring. Детерминистические локальные сети предоставляют администратору широкие возможности при определении максимального интервала времени, в течение которого кадр данных может находиться в передаче.

Основное отличие заключалось в том, что сети Token Bus использовали не кольцевую, а шинную топологию.

Стандарт Token Bus не нашел своей поддержки на рынке. Его применение

было ограничено в основном промышленными технологическими линиями. Однако шинные топологии успешно применялись во множестве других форм. В двух начальных формах сетей Ethernet, 10Base2 и 10Base5, использовалась шинная топология реализуемая на коаксиальном кабеле. Шины также стали основной технологией при соединении системных компонентов и периферийных устройств во внутренней архитектуре компьютеров.

2.2.2. Кольцевая и комбинированная топология

Кольцевая топология начала свое существование как простая одноранговая локальная сеть. Каждая сетевая рабочая станция соединялась с двумя ближайшими соседями (рис. 2.5. а, б). Схема такого соединения напоминала петлю или кольцо. Данные передавались по кольцу в одном направлении. Каждая рабочая станция функционировала как повторитель, принимая и отвечая на адресованные ей пакеты и передавая остальные пакеты следующей рабочей станции в кольце.

В первоначальной кольцевой топологии использовались одноранговые соединения между рабочими станциями локальной сети. Эти соединения обязательно должны были быть замкнутыми, т. е. формировать кольцо. Преимуществом таких сетей являлось легко предсказуемое время передачи. Чем больше устройств входило в кольцо, тем больше была задержка передачи. Недостаток кольцевой топологии в том, что при выходе из строя одной рабочей станции полностью отключается вся сеть.

Эти примитивные версии кольцевой топологии были вытеснены новой топологией IBM Token Ring, стандартизованной впоследствии в стандарт спецификации IEEE 802.5. Token Ring отошла от одноранговых соединений в пользу повторяющего концентратора. Устранение конструкции однорангового кольца повысило устойчивость всей сети к отказам отдельных рабочих станций. Несмотря на свое название, сети Token Ring используют звездообразную топологию и циклический метод доступа.

В локальных сетях звездообразной топологии может использоваться циклический метод доступа. Сеть Token Ring, проиллюстрированная на рис. 2.6, демонстрирует топологию виртуального кольца, формируемого методом доступа по алгоритму циклического обслуживания. Сплошные линии соответствуют физическим соединениям, а пунктирные линии обозначают направление логического потока данных.

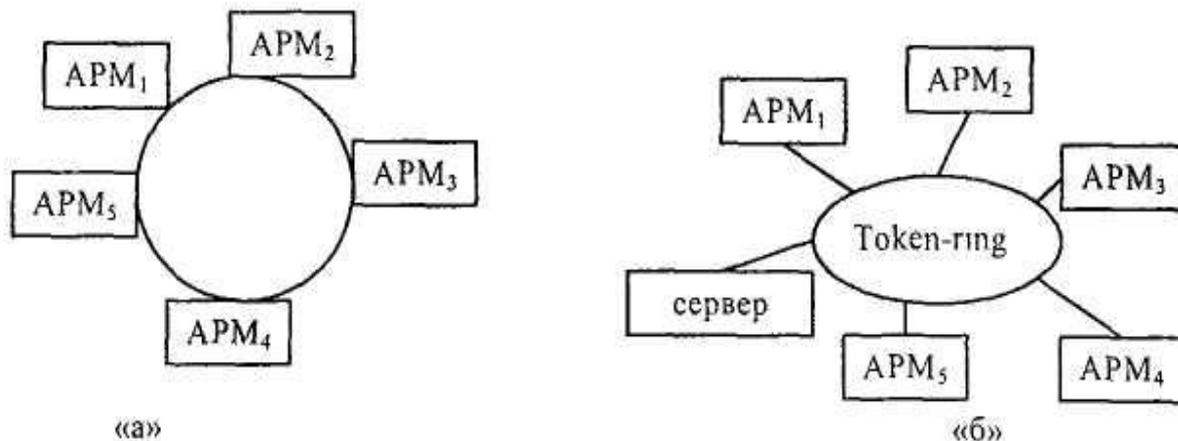


Рис 25 Кольцевые топологии петля (а) и кольцо (б)



Рис 26 Комбинированная топология сети Token Ring

Несмотря на то, что с технической точки зрения все устройства подключены к одному концентратору, маркер доступа в циклической последовательности обходит все сетевые устройства. По этой причине многие относят сети Token Ring

к "логической" кольцевой топологии, хотя физически они построены в форме звезды. В действительности концентратор Token Ring, более правильно называемый модулем многостанционного доступа (MSAU), организует физическое кольцо на электронном уровне.

2.2.3. Звездообразная топология

Локальные сети звездообразной топологии объединяют устройства сети, которые как бы расходятся из общей точки-концентратора (рис. 2.7). В отличие от кольцевых топологий - физических или виртуальных - каждое сетевое устройство в звездообразной топологии может обращаться к среде передачи независимо. Такие устройства вынуждены совместно использовать доступную полосу пропускания концентратора. Примером локальной сети звездообразной топологии служит сеть Ethernet 10 BaseT.



Рис. 2.7. Звездообразная топология.

Звездообразные топологии стали ведущим типом топологий в современных локальных сетях. Причиной такой популярности стала их гибкость, расширяемость и относительно невысокая стоимость по сравнению с более сложными локальными сетями со строго регламентируемыми методами доступа к среде передачи данных. Звездообразная топология не только сделала шинные и кольцевые топологии принципиально устаревшими, но и сформировала основу для создания новой топологии локальных сетей коммутируемой.

2.2.4. Коммутируемая топология

Коммутатор является многопортовым устройством канального уровня (второго уровня эталонной модели OSI). Коммутатор "изучает" MAC-адреса (Media Access Control - управление доступом к среде) и сохраняет их во внутренней таблице поиска. Коммутатор устанавливает временное соединение между отправителем и получателем кадра, и кадр передается по этому временному соединению (рис. 2.8).

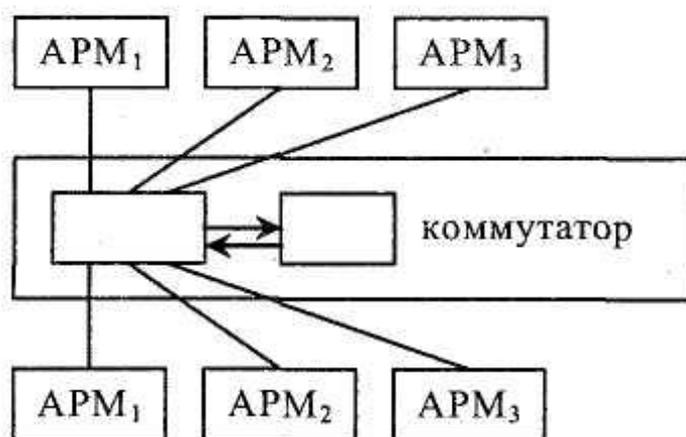


Рис. 2.8. Коммутируемая топология.

Схема локальной сети с коммутируемой топологией проиллюстрирована на рисунке 2.8. В этой схеме используется множество соединений с коммутирующим концентратором. Каждый порт и подключенное к нему устройство получает собственную полосу пропускания. Хотя первые коммутаторы передавали кадры по результатам анализа их MAC-адресов, в последующем технологический прогресс вскоре внес свои коррективы. Современные концентраторы в состоянии обрабатывать ячейки, кадры и даже пакеты, используя адреса третьего уровня (например, IP-адреса).

Кадр - это структура переменной длины, которая содержит данные, адреса отправителя и получателя и другие поля данных, необходимые для пересылок

данны на втором уровне эталонной модели (ЭМ) OSI. Ячейки (или контейнеры ячеек) похожи на кадры за исключением того, что их размер фиксирован. Пакеты состоящие из кадров это конструкции протоколов, функционирующих на третьем уровне модели OSI. Протоколы IP и IPX служат примерами протоколов третьего уровня, которые используют пакеты для инкапсуляции кадров данных перед транспортировкой их в виде внешних доменов.

Коммутаторы повышают производительность локальной сети двумя способами. Первый способ заключается в расширении полосы пропускания, доступной для всей сети. Например, коммутирующий концентратор Ethernet с 8 портами обслуживает 8 отдельных конфликтных доменов по 10 Мбит/с каждый, обеспечивая тем самым суммарную пропускную способность 80 Мбит/с.

Второй способ повышения производительности локальной сети состоит в сокращении количества устройств, которые вынуждены делить один сегмент полосы пропускания. Каждый выделенный коммутатором конфликтный домен реализуется двумя устройствами: собственно сетевым устройством и портом коммутатора, к которому он подключен. Эти два устройства могут полностью использовать все 10 Мбит/с своего сегмента полосы пропускания. В сетях, которые не поддерживают конкурирующие методы доступа к среде передачи (например, Token Ring), область циркуляции маркера ограничена намного меньшим количеством сетевых устройств, чем в сетях с конкурирующими методами доступа.

Открытым вопросом остается изоляция трафика в больших коммутируемых сетях. Приемлемая производительность достигается исключительно благодаря сегментации конфликтных, но не передающихся доменов. Чрезмерно насыщенный трафик передачи может существенно снизить производительность локальной сети.

Сложные топологии являются расширениями и/или комбинациями основных топологий физического уровня ЭМ OSI.

Основные топологии сами по себе применимы только в очень маленьких локальных сетях. Возможность расширения сетей основных топологий крайне

ограничена. Сложные топологии состояются из таких строительных блоков, которые позволяют формировать подходящую для конкретного случая новую расширенную топологию.

2.2.5. Последовательные цепочки

Простейшей из сложных топологий является та, где последовательно соединяются все концентраторы сети (рис. 2.9). Такая схема получила название последовательной цепочки. Для соединения задействованных в сеть концентраторов предполагается использовать их же порты. Таким образом, при реализации этой топологии не возникает никаких дополнительных расходов.

Маленькие локальные сети можно расширять, просто соединяя концентраторы в последовательную цепочку. Последовательную цепочку легко построить, для ее администрирования не требуется специальных навыков. Исторически сложилось так, что именно эта топология чаще всего использовалась для объединения локальных сетей первого поколения.

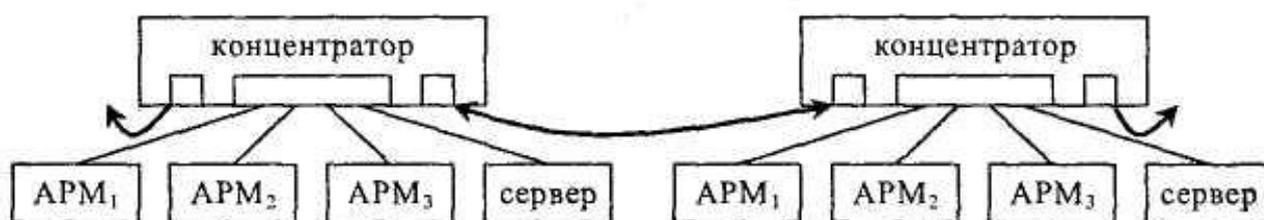


Рис. 2.9. Топология последовательных цепочек.

Недостатки топологии последовательных цепочек

Спецификации локальных сетей, в частности 802.3 Ethernet, определяют максимальный размер локальной сети, ограничивая количество концентраторов и/или повторителей, которые можно объединить в последовательную цепочку. Максимальный размер сети определяется ограничениями на расстояние, наложенными физическим уровнем, в сочетании с количеством устройств. Этот

размер называется максимальным диаметром сети. Превышение этого диаметра может привести к нарушению нормального функционирования локальной сети. Максимальный диаметр сети часто ограничивает количество концентраторов, которые можно соединить в цепочку. Это особенно относится к таким современным высокопроизводительным локальным сетям, как Fast Ethernet, которые накладывают жесткие ограничения на диаметр сети и количество соединенных вместе повторителей.

Повторитель - это устройство, которое принимает входящие сигналы, усиливает их до необходимого уровня и помещает обратно в сеть. Обычно функции усиления и повторения сигналов выполняют концентраторы. Следовательно, эти два понятия (повторитель и концентратор) можно использовать взаимозаменяемо.

Если в сети с топологией последовательной цепочки используется конкурирующий метод доступа к среде передачи, то проблемы могут возникнуть задолго до достижения максимального диаметра сети. Последовательная цепочка увеличивает количество соединений и, следовательно, количество устройств локальной сети. При этом суммарная полоса пропускания и количество доменов конфликтных сегментов остаются прежними. Последовательная цепочка просто увеличивает количество компьютеров, совместно использующих доступную полосу пропускания. Слишком много устройств, конкурирующих за одну и ту же полосу пропускания, создают много конфликтных ситуаций и могут быстро загнать сеть в тупик.

Эту топологию рекомендуется использовать в локальных сетях с небольшим количеством концентраторов и в небольших глобальных сетях.

2.2.6. Иерархическая топология

В иерархических топологиях используется более одного уровня концентраторов. Каждый уровень выполняет свои сетевые функции. На концентраторы нижнего уровня возлагается задача поддержки соединения с

пользовательскими станциями и серверами. Узлы более высоких уровней объединяют узлы пользовательского уровня. Проще говоря, множество концентраторов пользовательского уровня соединено с меньшим количеством концентраторов более высокого уровня. В данном случае концентраторы сами по себе остаются идентичными -единственное отличие заключается в способе их применения. Иерархические топологии лучше всего подходят для локальных сетей среднего и большого размера, в которых предполагается дальнейшее расширение и увеличение трафика.

Иерархические кольца

Сети, в которых реализована кольцевая топология, можно расширить путем иерархического соединения нескольких колец (рис. 2.10). Соединения с пользовательскими станциями и серверами могут поддерживаться множеством колец ограниченного размера, необходимых для обеспечения приемлемой производительности. Для соединения всех колец пользовательского уровня и организации доступа к глобальной сети может использоваться кольцо второго уровня - Token Ring.

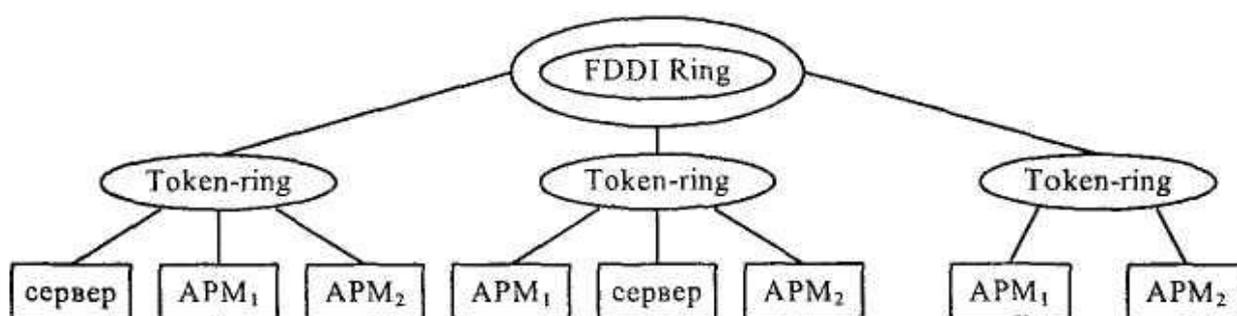


Рис. 2.10. Топология иерархии колец.

Небольшие локальные сети кольцевой топологии можно расширить, иерархически соединив несколько колец. На рисунке 2.10 две различные сети Token Ring с производительностью 16 Мбит/с (показанные как логические кольца) используются для соединения пользовательских станций, а отдельные кольца FDDI соединяют серверы и устройства магистрального уровня.

Иерархические звезды

Звездообразные топологии также можно реализовать, иерархически объединив несколько звезд (рис. 2.11). Иерархические звезды могут состоять из одного конфликтного домена или разделяться с помощью коммутаторов, маршрутизаторов, концентраторов или мостов на несколько конфликтных доменов.



Рис. 2.11. Топология иерархии звезд.

Конфликтный домен состоит из устройств, которые конкурируют за право передачи в совместно используемой среде. Коммутаторы, мосты и маршрутизаторы сегментируют конфликтные домены - создают несколько конфликтных доменов меньшего размера.

В топологии иерархической звезды один уровень организуется для соединения с пользователями и серверами, второй уровень функционирует в качестве общей магистрали передачи данных.

Иерархические комбинации

Общую производительность сети можно повысить, если не пытаться удовлетворить все функциональные требования единственным решением. Современные высокоуровневые коммутирующие концентраторы позволяют объединить несколько технологий. Для поддержки новой топологии достаточно просто вставить соответствующую плату в слот концентратора. Иерархическая топология представляет собой комбинацию различных топологий.

2.2.7. Топология беспроводных сетей

Беспроводная сеть с явно выраженной статической топологией исключает непосредственную связь периферийных станций (узлов). Связь между ними осуществляется через точки доступа (рис. 2.12). Точки доступа могут играть роль мостов, связывающих несколько сетей, беспроводных или кабельных. Несколько физически разделенных сетей, объединенных таким образом, могут¹ составить одну сеть на логическом уровне.



ТД – точка доступа

АРМ – автоматизированное рабочее место

Рис. 2.12. Пример топологии трёх беспроводных сетей со статической структурой.

Рисунок 2.12 иллюстрирует объединение трех беспроводных сетей посредством их точек доступа и проводной сети. Радиус действия такой сети гораздо больше, чем физическое радиопокрытие каждой БЛВС в отдельности. Прототипом БЛВС с инфраструктурой являются локальные кабельные сети Ethernet, имеющие звездообразную топологию, обеспечивающую полноценное управление, сетью. Все функции управления в сети возлагаются на базовую станцию. Точка доступа регулирует информационные потоки, определяет

качество связи и пропускную способность каждого узла. Сети с инфраструктурой поддерживают протоколы множественного доступа с обнаружением несущей и избеганием конфликтов, т. е. ситуаций, когда две периферийные станции пытаются начать передачу одновременно. Постоянная (статическая) функциональная структура с определенной топологией характерна не только для кабельных сетей. Системы мобильной сотовой телефонной связи, спутниковой телефонной связи построены по такому же принципу. Статическая природа этих сетей не позволяет проявиться всем возможностям, которые могли бы обеспечить беспроводные сети. Беспроводные мобильные сети позволяют отказаться от использования точки доступа - базовой станции, управляющей механизмом доступа к среде обмена. Узлы сети могут устанавливать непосредственную связь между собой. С помощью такого режима можно построить разветвленную беспроводную сеть с различной топологией, гибко изменять функциональную структуру, быстро перенастраивать сценарии связи и обмена информацией (например, быстро организовать конференцсвязь максимально большого числа узлов сети). На рис. 2.13 изображены две мобильные сети, каждая из них состоит из трех узлов. Если узлы находятся в пределах радиовидимости, возникает среда обмена информацией. Связь между узлами разных сетей невозможна, так как узлы одной сети находятся вне досягаемости узлов другой.

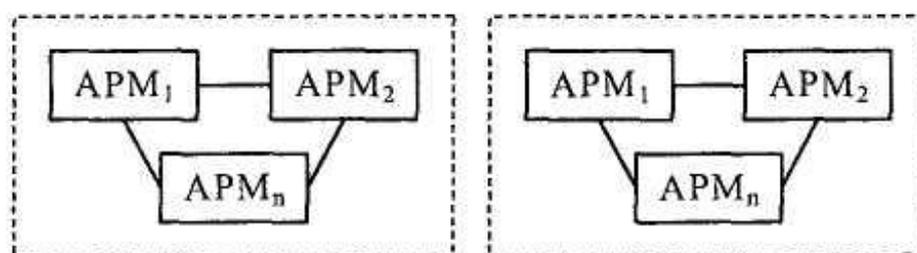


Рис. 2.13. Пример топологии двух мобильных беспроводных сетей.

Адаптеры беспроводной связи в узлах мобильной сети гораздо сложнее с функциональной точки зрения, так как должны обеспечить доступ к среде передачи данных, приемлемый уровень качества связи, предупреждение возможности возникновения изолированных узлов. На практике сети

рассматриваемых классов редко применяются в чистом виде. Обычно БЛВС являются смешанными и имеют свойства, характерные для каждого класса сетей. Базовые станции, являющиеся точками доступа, управляют средой обмена. В то же время возможна прямая связь узлов сети между собой. Некоторые узлы эпизодических сетей могут выполнять функции ретрансляторов. Остальные узлы связываются с ними, когда необходим обмен с узлами, находящимися за пределами досягаемости радиосвязи. Из рассматриваемых в данной главе БЛВС сети стандарта IEEE802.11 (рис. 2.14) и HIPERLAN IEEE 802.16 (рис. 2.15) являются типичными сетями с выраженной функциональной структурой, но в то же время они поддерживают мобильное (эпизодическое) соединение. Сети стандарта HIPERLAN нельзя однозначно отнести к сетям с фиксированной инфраструктурой, но на практике они обычно имеют явно выраженную топологию.



Рис. 2.14. Топология сети IEEE 802.11 с статической структурой.

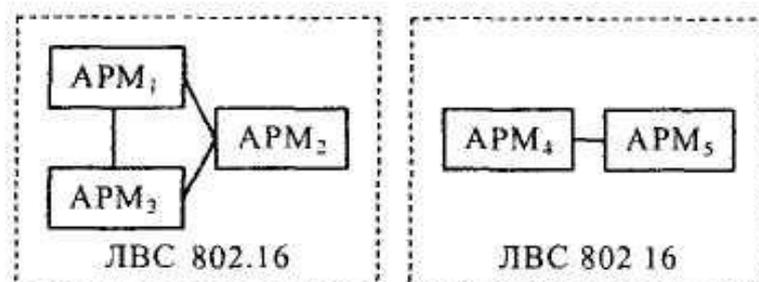


Рис. 2.15. Топология беспроводных сетей IEEE 802.11 с мобильной (эпизодической) структурой.

2.3. Коммуникационные компоненты локальных сетей

В настоящее время основными коммуникационными компонентами являются мосты, концентраторы и коммутаторы для локальных сетей.

Соответствие коммуникационных средств локальных сетей уровням семиуровневой модели взаимодействия открытых систем показано на рисунке 2.16.

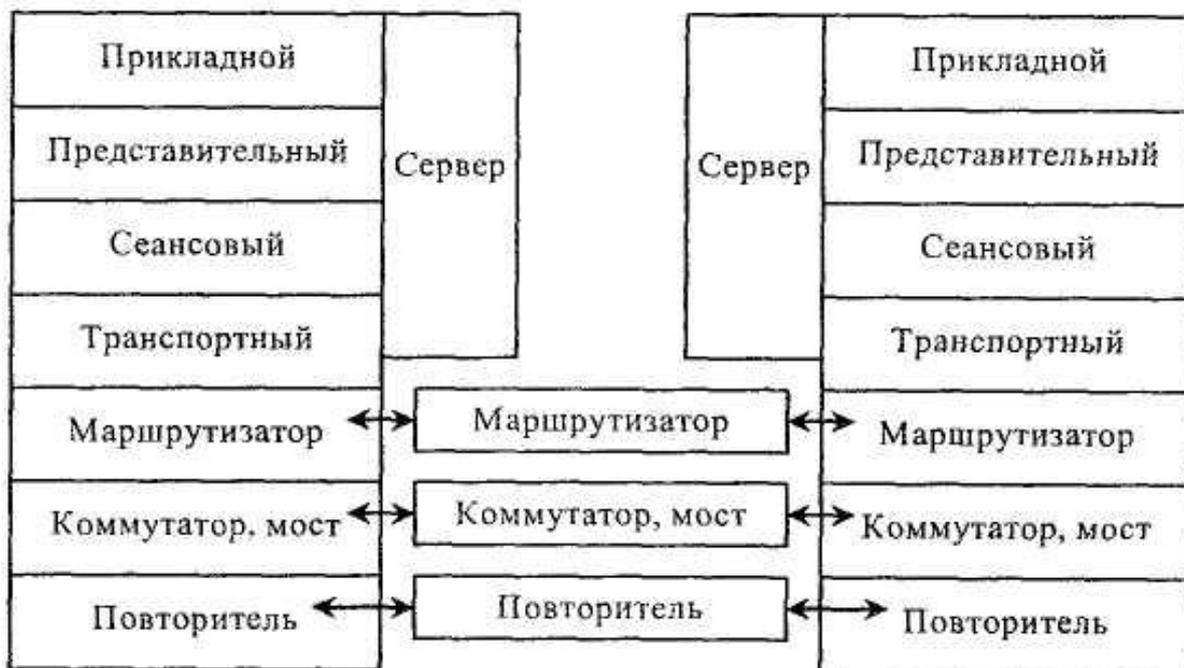


Рис. 2.16. Диаграмма сопряжения интерфейсов.

2.3.1. Мосты

Ниже приведены общий обзор мостов и описание способов их работы, включая маршрутизацию от источника с функциями моста или "прозрачного" устройства. Достаточно подробно описан алгоритм "охвата деревьев", используемый мостами для автоматического создания таблиц маршрутизации, списка возможных маршрутов данных и обновления этих таблиц при каждом изменении топологии сети.

Определение мостов

Мосты, областью действия которых является канальный уровень, объединяют две локальные сети и передают кадры в соответствии с присвоенными MAC-адресами. Мосты являются своего рода "низкоуровневыми маршрутизаторами".

Если удаленный мост по относительно медленному каналу (например, телефонной линии) устанавливает соединение между двумя локальными сетями, локальный мост устанавливает соединение между двумя смежными локальными сетями (рис. 2.17). При выборе локального моста основное внимание следует уделить производительности, в то время как для удаленного моста критической характеристикой является возможность передачи данных по линии значительной длины.

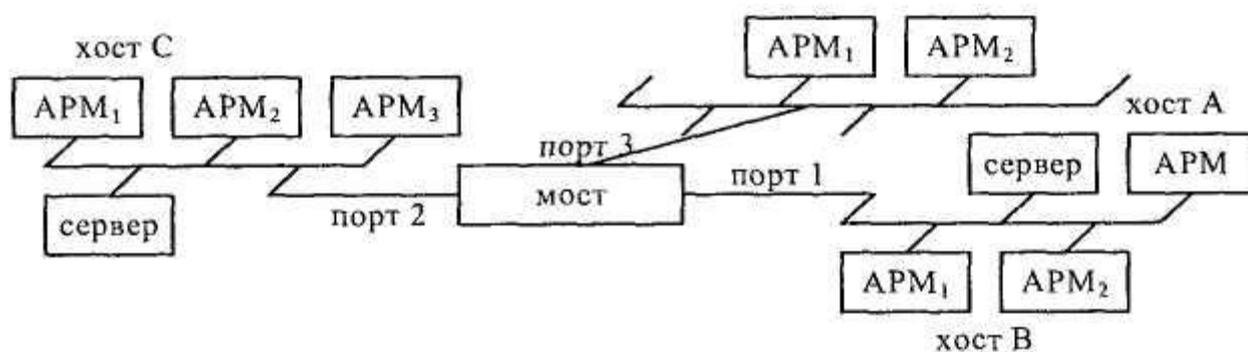


Рис. 2.17. Топология сопрягаемых сетей с помощью моста интерфейса.

Сравнительный анализ мостов и маршрутизаторов

Мосты не имеют ни малейшего понятия о протоколах более высоких уровней, инкапсулированных в передаваемые кадры. Следовательно, мосты будут абсолютно одинаково (и одновременно) обрабатывать протоколы IP, IPX, как и любые другие. Кроме того, мосты позволяют сегментировать сети, которые используют не поддерживающие маршрутизацию протоколы (например, NetBEUI).

Тот факт, что маршрутизаторы обрабатывают данные на сетевом уровне, в значительной степени облегчает установление соединений между различными канальными уровнями, например, между сегментами Token Ring и Ethernet.

Довольно часто управление мостами оказывается намного сложнее управления маршрутизаторами. Протоколам типа IP свойственны "изохронные" протоколы маршрутизации, позволяющие сетевому администратору пристально следить за процессом маршрутизации. Протоколы семейства IP предоставляют некоторую дополнительную информацию, упрощающую задачу логической сегментации (такую информацию можно найти даже в самих адресах). Мосты по своей природе сложнее поддаются управлению - в этом нет ничего удивительного, поскольку они оперируют исключительно с MAC-адресами и на физическом уровне топологии сети. Именно поэтому рекомендуется использовать мосты в небольших простейших сетях.

Существует два типа мостов:

- Прозрачные мосты: как правило, используются для установления соединения между сегментами Ethernet.
- Мосты с маршрутизацией от источника: как правило, используются для установления соединения между сегментами Token Ring.

Прозрачные мосты

Прозрачные мосты чаще всего используются для установления соединений между сегментами Ethernet. Мост ретранслирует трафик между различными сегментами и одновременно изолирует локальный относительно сегмента

получателя трафик. Таким образом снижается интенсивность трафика сети. В качестве устройств сопряжения с сетью мост использует два и более порта.

Простейший режим функционирования моста возможен только в том случае, если в сети отсутствуют кольца, а между двумя хостами можно установить соединение единственным способом.

Мост не зря называется прозрачным, поскольку он невидим для всех хостов сети. С точки зрения сетевого уровня (например, протокола IP) все сети, соединение между которыми установлено с помощью мостов, можно считать физическими соединениями.

Каким образом поддерживается эта "прозрачность"? Основной функцией моста является передача полученных кадров. Единственным исключением является ситуация, когда полученный кадр предназначен устройству, хост которого подключен к тому же порту, что и хост отправителя (например, полученный первым портом кадр необходимо отослать через этот же порт). Определяя подобную ситуацию, мост в состоянии в значительной степени сократить количество ретрансляций.

Для каждого порта моста составляется список MAC-адресов устройств, подключенных к данному порту. Мост будет знать, что хост G подключен к третьему порту, если третий порт получит кадры от хоста G. На случай, если хост изменит свое расположение в сети, каждая запись списка обновляется через определенное время. Каждый раз после получения кадра с известного MAC-адреса соответствующий счетчик запускается заново.

В простейшем случае мост соединяет две подсети. На рисунке 2.17 мост должен передавать кадры от хоста А к хосту С, но ни в коем случае не от хоста А к хосту В.

Однако в начальной стадии определения конфигурации ситуация далеко не так проста, как кажется. Представьте, что мост только что начал функционировать. Все таблицы данных незаполнены - на данном этапе неизвестно, какому порту соответствуют какие хосты. По мере обработки трафика таблицы заполняются приблизительно следующим способом:

Таблицы моста: Порт 1 - «неизвестно»; Порт 2 - «неизвестно».

Хост А пересылает кадр хосту В. Мост получает кадр на первом порту, но не знает, где расположен хост В, поэтому передает кадр на второй порт. В таблицу первого порта мост добавляет запись о хосте А.

Таблицы моста: Порт 1 - «А»; Порт 2 - «неизвестно».

Хост В посылает ответное сообщение хосту А. Мост получает кадр на первом порту, но не транслирует его во второй порт, поскольку теперь достоверно известно о том, что хост А также подключен к первому порту. Мост обновляет таблицу для первого порта, добавляя к ней запись для хоста В.

Таблицы моста: Порт 1 - «А, В»; Порт 2 - «неизвестно».

Хост А посылает кадру хосту В. Мост получает кадр на первом порту, но на этот раз уже располагает информацией о том, где расположен хост В (также на первом порту), поэтому кадр не транслируется во второй порт. Счетчик TTL для записи хоста А будет перезапущен.

Таблицы моста: Порт 1 - «А, В»; Порт 2 - «неизвестно».

На рис. 2.18 приведена архитектура взаимосвязей (интерфейсов) БЛВС с помощью моста IEEE802.il.



Рис. 2.18. Протокольная архитектура мостов IEEE 802.11.

2.3.2. Концентраторы

В процессе разработки оптимальной сетевой среды для заданной архитектуры специалисту придется принять ряд ответственных решений. Одним из самых важных решений является выбор топологии сети. Приходится учитывать абсолютно все факторы: предполагаемые по каждому уровню архитектуры производительности и надежности, мероприятия администрирования и профилактики, возможность и способ расширения сети, с учетом ущерба, который может нанести бюджету развертывание спроектированной сети.

Во многих случаях сложность решения задач о необходимости приобретения концентраторов с учетом расширения заставляет администратора отказаться от создания сети типа стандарта 10base-T. Вместе с тем, стоит задача модернизации существующей локальной сети стандарта 10base-2, то дополнительные затраты на приобретение концентраторов не должны мешать проекту повышающему производительность и гибкость инфраструктуры, которые будут достигнуты в результате установки этих концентраторов.

В подтверждение выше изложенному, следует то, что концентратор являлись точкой сопряжения сетей, использующих звездообразную топологию. Arcnet, 10base-T и 10base-F (равно как и многие другие запатентованные сетевые топологии) интенсивно используются как для соединения различных кабелей, так и для распределения данных по различным сегментам сети. Концентраторы выступают в роли распространителей сигнала. Они снимают сигнал с одного порта и транслируют его на все остальные порты. Ряд концентраторов даже ухитряется усиливать слабый сигнал перед ретрансляцией. Другие изменяют временные характеристики сигнала с целью обеспечения действительно синхронного обмена данными между всеми портами. Концентраторы с несколькими разъемами типа 10base-F с помощью зеркал разделяют луч света, направляя его на различные порты.

На рисунке 2.19а показана одна из возможных конфигураций сети стандарта 10base-2. Обратите внимание на способ подключения машин между собой. Помните, что посланные первой системой данные должны быть

обработаны всеми системами, расположенными между отправителем и получателем.

На рисунке 2.196 показана та же сеть, что и на рисунке 2.19а, но построенная по стандарту 10base-T. Рисунок наглядно иллюстрирует различия в топологии, а также роль концентратора.

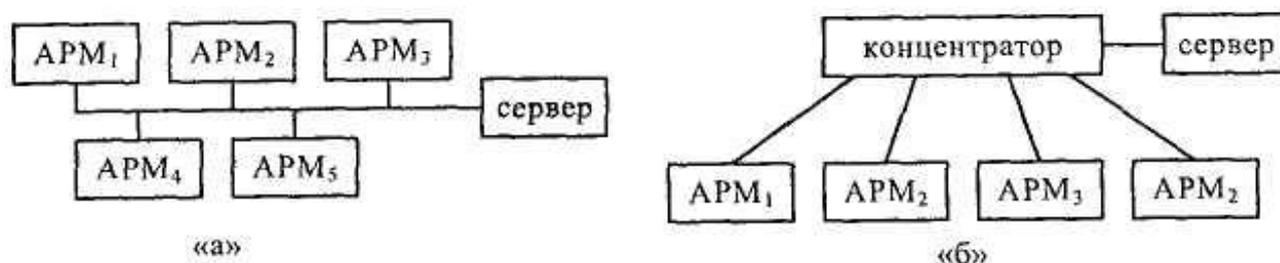


Рис. 2.19. Схема конфигураций сети.

Например, в соответствии со стандартом 10base-T все устройства должны быть физически подключены к одному или более концентраторам с помощью неэкранированного кабеля из витых пар. Поскольку концентратор имеет несколько портов (возможно, даже разнотипных), можно будет подключить много устройств. Иногда возникает необходимость соединить вместе несколько концентраторов. В этом случае с помощью высокоскоростных портов концентраторов вполне возможно организовать магистраль. Все концентраторы (а возможно, и сетевые серверы) должны быть подключены непосредственно к высокоскоростной магистрали. Поскольку в большинстве локальных сетей наиболее интенсивный трафик наблюдается между рабочими станциями и первичными серверами, магистраль сегмента будет оказывать существенное влияние на общую производительность сети.

На рисунке 2.196 магистраль соединяет несколько концентраторов и серверов непосредственно по выделенному каналу. Такой способ соединения идеально подходит для высокоскоростной сети Ethernet и других волоконно-оптических сетей.

Сети топологии "эстафетное кольцо" также имеют устройства, которые можно считать концентраторами. Устройство множественного доступа (УМД -

MSAU Multistation Access Unit) также рассматривается в качестве концентратора, поскольку выполняет те же функции, что и концентратор сетей Ethernet. Однако устройства множественного доступа с помощью механических ключей и реле последовательно адресуют пакеты всем активным устройствам - концентраторы сетей Ethernet выполняют те же действия параллельно.

Существует несложный способ определения необходимости использования концентратора в локальной сети. Если развертывается сеть звездообразной топологии из более чем двух машин, концентратор необходим. Однако у этого правила есть исключения. Если развертываемая сеть стандарта 10base-T объединяет только две машины, их можно будет соединить и без помощи концентратора. Однако придется воспользоваться специальным кабелем, соединяющим передающие контакты одной системы с принимающими контактами другой системы и наоборот. Кабели такого типа становятся все более распространенными. Если вы не сможете приобрести такой кабель, попробуйте сделать его самостоятельно. Для этого не нужны дорогие материалы - достаточно куска витого кабеля небольшой длины, двух разъемов RJ-45 и простейшего обжимного приспособления. В таблице 2.1 приведен способ распайки разъемов кабеля Ethernet для соединения двух систем без помощи концентратора. Созданный подобным образом кабель сети Ethernet часто называют кросскабелем.

В приведенной таблице 2.1 проиллюстрирован способ распайки разъемов кабеля сети Ethernet, позволяющий отказаться от использования концентратора для соединения двух машин. Если возникнет необходимость подключения третьей машины, придется-таки использовать и концентратор, и два кабеля 10base-T.

Таблица 2.1.

***Распайка разъемов кабеля сети Ethernet,
позволяющая соединять две системы
без помощи концентратора***

Первый разъем RJ-45		Второй разъем RJ-45	
Номер контакта	Функция	Номер контакта	Функция
1	Передача +	3	Прием +
2	Передача -	6	Прием -
3	Прием +	1	Передача+
6	Прием -	2	Передача -

Предназначение концентраторов

Концентраторы являются критическим звеном сети звездообразной топологии. Существуют различные типы концентраторов, каждый из которых предоставляет определенные функциональные возможности. Ниже будут рассмотрены и общие свойства концентраторов, и различия между пассивными, активными и интеллектуальными концентраторами, а также о некоторые дополнительные функциональные возможности современных высокопроизводительных концентраторов.

Все концентраторы обладают стандартным набором функциональных возможностей, которые частично определены типом используемого кабеля. Во многих отношениях концентратор является обычным сетевым устройством, которое должно соответствовать стандартным параметрам сети, в которой оно функционирует. Независимо от того, что концентраторы занимают более привилегированное положение по сравнению с обычными устройствами сопряжения, на них накладываются те же ограничения стандартов IEEE.

Большинство соединений с концентратором осуществляется с помощью разъемов RJ-45, которые являются стандартным соединителем во многих сетях Ethernet, использующих проводку из витых пар. Все стандарты от 10base-T до 100base-T используют в качестве проводки между рабочими станциями, принтерами, другими устройствами локальной сети и концентратором один из типов витого кабеля. На концах кабелей обязательно расположены разъемы RJ-45.

Разъем RJ-45 очень похож на обычный телефонный разъем. Единственное различие в том, что разъем первого типа немного шире. Разъемы RJ-45 используются для соединения витым кабелем устройств не только в сетях Ethernet, но и в сетях Token Ring.

Длина кабеля, который может быть подведен к концентратору, ограничена свойствами среды передачи (табл. 2.2). Например, длина кабеля 10base-T не может превышать 100 метров. Это ограничение продиктовано спецификациями стандарта 10base-T комитета IEEE, а не причудами конкретного концентратора. Например, если концентратор с помощью разъема 10base-F предполагается

подключить к высокоскоростной магистрали, он не может быть удален от магистрали более чем на 2 километра - это определено спецификациями IEEE для 10base-F.

В таблице 2.2 перечислены соответствующие различным стандартам Ethernet максимальные длины кабелей. Имейте в виду, что в случае необходимости длину кабеля можно увеличить с помощью повторителей сети Ethernet.

Таблица 2.2.

***Определенная спецификациями IEEE
максимальная длина кабелей различных
стандартов Ethernet***

Тип Ethernet	Максимальная длина
10base-2	185 метров
10base-5	500 метров
10base-T	100 метров
10base-F	2 километра
10broad-36	3 600 метров

Естественно, существуют и другие стандартные требования. Поскольку концентраторы являются электронными устройствами, которые принимают сигнал и ретранслируют его на несколько портов, для их работы необходим источник питания. Большинство концентраторов оборудованы светодиодами, с помощью которых можно отслеживать состояние устройства. Чаще всего светодиоды предоставляют информацию о напряжении питания и осуществлении передачи данных через определенные порты. Некоторые концентраторы оборудованы дополнительными светодиодами, позволяющими отслеживать трафик через определенные порты, а также возникновение конфликтов пакетов в локальной сети.

Пассивные концентраторы

Пассивные концентраторы являются довольно безучастными к данным, передаваемым устройствами, полностью подтверждающими свое название. Такие концентраторы лишь незначительно повышают производительность локальной сети и никоим образом не облегчают поиск вышедшего из строя оборудования или узкого места системы. Они просто транслируют полученные пакеты во все порты, выполняя простейшую функцию концентратора.

Как правило, в дополнение к разъемам RJ-45 пассивные концентраторы оборудованы одним портом 10base-2. Известно, что стандарт 10base-5 соответствует Ethernet 10Мбит/с с проводкой из толстого коаксиального кабеля. Этот разъем 10base-2 используется для подключения к магистрали сети. Другие, более современные пассивные концентраторы оборудованы портами АШ, которые можно соединить с ретранслятором и создать более производительную магистраль.

Большинство пассивных концентраторов являются великолепными устройствами начального уровня, которые предпочтительно использовать в случае развертывания небольших сетей Ethernet звездообразной топологии. Их использование в случае перехода от стандарта 10base-2 к недорогому 10base-T позволит в значительной степени повысить производительность, затратив при этом минимум средств.

Активные концентраторы

Активные концентраторы, помимо обычной ретрансляции данных, выполняют и некоторые другие действия. Как правило, они поддерживают функциональные возможности пассивных концентраторов и дополнительно проверяют доставку по назначению отосланных данных. Активные концентраторы играют более значимую роль в сетях Ethernet, поскольку поддерживают так называемую технологию передачи с промежуточным накоплением, в соответствии с которой концентраторы анализируют полученные данные перед их ретрансляцией. Это не значит, что концентратор присваивает пакетам данных различные приоритеты - просто предпринимается попытка

восстановить "поврежденные" пакеты и одновременно изменить время доставки других пакетов.

Если активный концентратор получил слабый, но четкий сигнал, перед ретрансляцией сигнал будет усилен до необходимого уровня. Эта функциональная возможность позволяет использовать в сети устройства, параметры сигнала которых отличаются от оптимальных. Если сигнал определенного устройства принципиально игнорируется другими устройствами сети, которые подключены через пассивные концентраторы, усиление сигнала с помощью активного концентратора позволит оставить устройство в составе локальной сети. Кроме того, некоторые обладающие функциональными возможностями диагностики активные концентраторы позволяют находить вышедшие из строя устройства.

Активные концентраторы также позволяют изменять порядок доставки принятых пакетов. Некоторые кабели подвержены влиянию электромагнитных помех, которые мешают своевременному получению пакетов концентратором или устройством на другом конце кабеля. В других ситуациях пакеты могли бы не попасть к получателю вообще. Активные концентраторы позволяют компенсировать потерю данных, ретранслируя для этого пакеты только на соответствующие порты и изменяя одновременно временные характеристики для более медленной доставки пакета по зашумленному каналу. Несомненно, подобная процедура снижает производительность всех подключенных к концентратору устройств, но иногда с этим можно мириться - особенно в том случае, когда в результате изменения временных характеристик снижается количество конфликтов в локальной сети. Если не придется слишком часто ретранслировать потерянные данные, сеть будет в состоянии обрабатывать больше новых запросов на обслуживание. В очередной раз обращаем ваше внимание на тот факт, что активные концентраторы упрощают поиск проблемных кабелей, обозначая порт, данные которого постоянно приходится ретранслировать.

Активные концентраторы в некоторой степени повышают

производительность сети и в некоторых случаях облегчают задачу поиска проблемного оборудования. Активные концентраторы имеют более высокую стоимость по сравнению с пассивными. Наиболее целесообразно использовать их в сложных конфигурациях.

Интеллектуальные концентраторы

Интеллектуальные концентраторы имеют массу преимуществ по сравнению с пассивными и активными. В архитектурах тех сетей, которые предполагают модернизировать сеть таким образом, чтобы пользователи получили возможность наиболее эффективно использовать ресурсы сети, должны быть введены интеллектуальные концентраторы. Подобные устройства появились совсем недавно и поэтому еще не столь популярны. Тем не менее интеллектуальные концентраторы уже доказали свое право на существование как технология, позволяющая в значительной степени повысить производительность локальной сети.

В дополнение ко всем преимуществам активных концентраторов включение интеллектуальных устройств в сетевую инфраструктуру предоставит возможность управлять сетью из центральной точки. Если с любым подключенным к интеллектуальному концентратору устройством возникнут проблемы, их можно будет с минимальными усилиями идентифицировать и исправить с помощью предоставленной интеллектуальным концентратором информации. Более того, предварительно концентратор попытается устранить проблему самостоятельно. Это уже большое достижение по сравнению со стандартными активными концентраторами. Процесс поиска неисправности в большой корпоративной сети без инструмента централизованного управления обычно превращается в бестолковую беготню между кабельными коробками в поисках некорректно функционирующего устройства.

Еще одним значительным преимуществом интеллектуальных концентраторов является возможность работы с устройствами, которые поддерживают различную скорость передачи данных. Естественно, интеллектуальные концентраторы оборудованы дополнительными портами, позволяющими подключиться к высокоскоростной магистрали - это общая черта

всех концентраторов. Однако интеллектуальные концентраторы поддерживают стандартные скорости передачи данных 10,16 и 100 Мбит/с между настольными системами, использующими стандартные топологии сетей Ethernet и Token Ring. Это обуславливает возможность постепенного повышения скорости передачи данных в сети от 10 Мбит/с до 100 Мбит/с, а также возможность пересылки информации устройствам с максимальной скоростью.

В дополнение ко всему вышесказанному, нужно добавить, что с целью повышения гибкости и облегчения управления разнородной сетью, состоящей из различных сред передачи и отличающихся по уровню технологии сегментов, интеллектуальные концентраторы обеспечивают.

1. Возможности поддержки других устройств, например, терминальных серверов, мостов, маршрутизаторов и коммутаторов.

2. Поставку современного интеллектуального и универсального программного обеспечения, предназначенное для управления сетью и имеющее несложный интерфейс, что делает их основным компонентом большинства универсальных систем управления ресурсами сети.

Существует достаточно много дополнительных функциональных возможностей, которые поддерживаются современными концентраторами различных изготовителей. Для функционирования некоторых концентраторов необходимо несколько источников переменного тока. В случае выхода из строя одного из источников, его нагрузка распределяется между остальными, и устройство продолжает функционировать. Другие концентраторы имеют встроенные источники постоянного напряжения и будут задействованы в случае отключения внешнего питания. Запасные вентиляторы некоторых концентраторов продолжают охлаждать устройство в случае выхода из строя основных. Большинство интеллектуальных концентраторов автоматически согласуют оконечные сопротивления коаксиальной проводки, позволяют оперативно заменять модули, а также автоматически подстраиваются под полярность неправильно проложенной проводки 10base-T. Некоторые

интеллектуальные концентраторы резервируют средства синхронизации и хранения данных конфигурации. Резервирование средств синхронизации позволяет концентратору постоянно арбитраживать процесс своевременной доставки пакетов. Резервирование средств хранения конфигурации позволяет интеллектуальным концентраторам присваивать портам различные параметры. В этом случае каждый концентратор сети должен хранить сведения о конфигурации другого концентратора, возвращая их по запросу. Кроме того, некоторые изготовители дополнительно поставляют предназначенные для выполнения задач маршрутизации и ретрансляции модули, которые интегрируются в корпус концентратора большой корпоративной сети.

Одним из наиболее интересных аспектов компьютерной индустрии являются темпы появления новых продуктов и усовершенствования существующих. Обслуживающий современные сети персонал должен быть в курсе всех новинок. В отличие от других индустрий, где на революционные изменения необходимо от пяти до пятнадцати (а иногда и больше) лет, в сетевой индустрии кардинальные изменения происходят максимум через полтора года - налицо логарифмическая зависимость. Среди причин такого безудержного роста, помимо очевидных факторов спроса, можно назвать необычайно большое количество изготовителей оборудования и разработчиков программного обеспечения, результатом чего является непрерывное совершенствование технологий. Поскольку сетевые технологии уже стали неотъемлемой частью мира бизнеса, нет ничего удивительного в том, с каким упорством создатели программного обеспечения и оборудования пытаются усовершенствовать свои продукты.

При выборе сетевого оборудования (причем совсем необязательно, что это будут именно концентраторы), необходимо обратить внимание на следующие факторы:

- ассортимент предлагаемых устройств;
- инструкции поддержки эксплуатации устройств;
- соотношение цена/функциональные возможности устройств.

Начав поиски идеального концентратора, можно найти множество изготовителей, многие из которых предложат практически аналогичные устройства. Если предполагается объединить в сеть всего несколько машин (скажем, до 12 машин), достаточно приобрести один из пассивных концентраторов, присутствующих на рынке. Если вы ставите перед собой задачу создания для рабочей группы большой, более современной сетевой инфраструктуры, к вопросу выбора оборудования придется подойти более взвешенно. Поиск изготовителя, предлагающего системы интеллектуальных концентраторов, которые можно использовать при развертывании сетей любого масштаба, а также другие устройства, в частности, маршрутизаторы, мосты и сетевые адаптеры, которые в состоянии функционировать в той же системе, представляет собой нелегкую задачу. Приобрести в местном магазине концентратор наобум не представит большого труда, но следует задуматься о перспективах такого поступка. Этот шаг особенно важен в том случае, если предполагается дальнейшее расширение сети или объединение существующих локальных сетей в комбинированную звездообразную топологию. Кроме того, многие изготовители специально оговаривают совместимость своих продуктов с однородной средой.

Крупнейшие изготовители через сеть сертифицированных дистрибьюторов предоставляют доступ к службе технической поддержки. Если перед вами стоит задача развертывания новой сети или модернизации существующей, а времени хватает только на то, чтобы оплатить счета, услуги подобных служб окажутся достаточно заманчивыми. Если же предполагается развернуть локальную сеть, которая не будет длительное время модернизироваться, вы ничего не потеряете в том случае, если выберете соответствующее вашим потребностям оборудование менее известного производителя. Но в этом случае рассчитывать на поддержку квалифицированного персонала уже не приходится. Придется консультироваться со своими коллегами, уже имеющими опыт в обращении с таким оборудованием. Вполне возможно, что общение с ними внесет коррективы в ваши планы. Имейте в виду, что только квалифицированный инженер поможет спроектировать сеть,

оптимальным образом соответствующую вашим требованиям.

Изделия многих известных изготовителей интеллектуальных концентраторов и другого оборудования значительно дороже аналогичных продуктов менее известных фирм. Нет ничего удивительного в том, что пассивные концентраторы начального уровня намного дешевле интеллектуальных, но разница в несколько сотен долларов между устройствами с абсолютно аналогичными характеристиками заставляет задуматься. Однако в зависимости от масштаба проекта или предполагаемой производительности локальной сети дополнительные расходы на аппаратные средства сохранят массу времени, денег и нервов в случае добавления новых сетевых узлов, расширения функциональных возможностей маршрутизирования, попытки устранить проблемы соединения, увеличения скорости вещания определенных систем и даже в повседневной эксплуатации сети. Обязательно следует учитывать то обстоятельство, что дополнительные расходы на оборудование позволят сэкономить средства при модернизации сети.

2.3.3. Особенности коммутационных технологий

Один из наиболее острых аспектов, характерных для вычислительных сетей конца 90-х годов, связан с интенсивным развитием информационно-коммуникационных технологий. Даже самые консервативные оценки свидетельствуют о появлении кардинальных изменений в области информационной технологической индустрии каждые 18 месяцев, а в некоторых случаях даже чаще! С недавнего времени компании ведут жесткую конкуренцию за место на рынке аппаратного и программного обеспечения, которое позволит с уверенностью вступить в 21-й век. Эти компании сумели добиться некоторого успеха благодаря разработке напичканных различными "полезными" модулями браузеров, самонастраивающихся операционных систем и собственных высокоскоростных модемов, а также оборудованию больших городов новейшими

каналами связи, включая линии ATM, ADSL и т. д.

Одним из неприятных факторов, связанных с интенсивным развитием сетевых технологий, является постепенное снижение объемов финансирования менеджеров и специалистов по сетям. С точки зрения пользователя, технически неосведомленного (особенно в том случае, если системные проблемы еще не приобрели хронический характер и надежность сети еще не пострадала), нет никакой необходимости дополнительно инвестировать десятки тысяч долларов для новых изысканий. В конце концов, если устройство работает, то зачем его ремонтировать? Очень редко разрабатываются долгосрочные планы профилактических мероприятий, позволяющих избежать многих проблем или хотя бы решить их с минимальными затратами.

К несчастью, столь легкомысленное отношение к этому вопросу ставит специалистов по сетям в весьма невыгодное положение. В финансовом отношении ваши руки связаны. Получение достаточного финансирования для поддержки в рабочем состоянии существующей сетевой инфраструктуры, усовершенствования проводки, аппаратного и программного обеспечения, столь необходимых постоянно растущему классу пользователей, уже можно считать мало реальным. А как бороться с задержками и перебоями в доставке данных, отключением устройств или возникновением конфликтов? Пользователь ничего не сможет с этим поделать до тех пор, пока на физическое расширение полосы пропускания, создание новых серверов и прием на работу тысяч специалистов не будут тратиться тысячи долларов. Но существует и более приемлемое решение - коммутация в сетях Ethernet.

Поскольку исполнительный менеджмент становится особенно скупым, как только речь заходит о финансировании поддержки, обслуживания и расширения сетевых ресурсов, придется достаточно часто сталкиваться с различными проблемами, которые потребуют новых нестандартных решений. Зачастую удастся лишь наметить план ближайших действий, а выделенные средства уже будут исчерпаны. Два фактора особенно ощутимо влияют на обслуживаемую вами сеть, поэтому придется уделять особое внимание им обоим. В противном

случае вы окажетесь меж двух огней.

Во-первых, компьютеры, рабочие станции и серверы уже не такие, какими они были раньше. Больше не существует настольных компьютеров в виде тупых терминалов или систем, интеллект которых немногим превышал интеллект среднего тостера. Класс современных настольных систем, рабочих станций и сетевых серверов намного мощнее и быстрее своих предшественников. Обычная современная машина обладает таким объемом памяти и производительностью процессора, что превосходит параметры многих машин класса "сервер", широко использовавшихся еще пять лет назад. В результате требования к машинам в значительной степени ужесточились. Во-вторых, одновременно появилась необходимость в создании систем, осуществляющих постоянную передачу данных по сети с целью обеспечения доступа к удаленным файлам, ресурсам Internet, совместного использования различных устройств и т.д.

Если все вышесказанное прозвучало как призыв к действию - вводите технологии профилактики и развития сетей! Если же это оставило вас равнодушным - работайте, пока не развалите вашу инфраструктуру окончательно! Поскольку сеть растет с точки зрения количества узлов, пользователей и предоставляемых услуг, рано или поздно возникнет главная проблема сетей - недостаточная пропускная способность. От этого, несомненно, будет страдать производительность сети, пользователи будут недовольны возникающими в работе задержками, приложения клиент/сервер будут медленно реализованы, а межсетевые соединения не смогут обрабатывать интенсивный трафик. Пожалуй, это не лучшим образом скажется на работе сети. Есть два выхода: продолжать работать без профилактического обслуживания сети, что сможет некоторое время поддержать функционирование сети, или использовать преимущества коммутации в сетях Ethernet с профилактикой и модификацией.

Необходимость использования мостов

Использование мостов с целью разделения нескольких сегментов сети долгое время считалось прекрасным способом снижения межсегментного трафика и одновременного повышения производительности растущей или устоявшейся

сети. Хотя использование мостов позволяет инженерам разделять насыщенные сети на более управляемые мини-сети, это решение не всегда оказывается эффективным. Зачастую складывается ситуация, когда у пользователей определенного сегмента возникает необходимость в установлении значительного количества внутрисегментных соединений. И тут становится очевидной неспособность этого метода устанавливать одновременные межсегментные связи, что наводит на мысль о нецелесообразности применения данного решения. К счастью, одним из достоинств коммутации является решение проблемы внутрисегментных соединений. Однако, несмотря на все вышесказанное, следует признать, что использование мостов в некоторых случаях более целесообразно, поэтому не стоит полностью отвергать этот метод. Если подсети предполагают установление ограниченного количества межсегментных соединений, полезными окажутся именно мосты.

В идеальном случае проблема критических заторов в сети никогда бы не возникла. Пользователи всегда располагали бы массой времени и избавлялись бы от всех проблем еще до их появления. Предположим, что компания недавно объединилась с конкурентами и теперь необходимо добавить 12000 узлов в существующую (и без того перегруженную) сеть архитектуры "эстафетное кольцо". Пожалуй, не стоит даже начинать заниматься этим гиблым делом без установки канала FDDI. Как только вы его установите, к зданию пристроят три этажа и компания наймет новых служащих. Так почему бы не вырвать старую проводку, проложить кабель 5-й категории и внедрить Fast Ethernet? Стандарты Fast Ethernet, ATM, FDDI и ADSL (в числе прочих) слишком дороги и требовательны к ресурсам для того, чтобы использовать их в качестве безотказного средства в борьбе с перегрузками сети. Все эти решения задач создания, внедрения и поддержки сети, базирующейся на новых технологиях, потребуют достаточного времени и усилий, поскольку задачи эти не из легких и без сомнения повлечет за собой дополнительные расходы на обучение персонала. Нечего и говорить о неизбежных простоях в переходный период, о дополнительных расходах, связанных с широкомасштабным внедрением новых

технологий, или любой из множества непредвиденных ситуаций, требующих немедленного решения.

Другой способ, который часто используют для борьбы с перегрузками в сети, заключается в использовании с целью разгрузки внутрисегментного трафика мостов и маршрутизаторов. Хотя это решение выглядит достаточно логичным, оно зачастую приводит к весьма незначительным результатам. Процедура конфигурации мостов и маршрутизаторов для обеспечения максимальной производительности требует большого профессионализма и тщательного анализа сетевого трафика.

В реальной жизни невозможно решить все сетевые проблемы путем постоянной модернизации. Трудно позволить постоянные траты на модернизацию вместе с потерей времени и другими издержками, если каждый раз придется искать простейший выход из создавшегося положения. Во многих случаях коммутация сетей Ethernet оказывалась ключевым решением в борьбе с перегрузками сетей подобного типа, позволяя сохранить, таким образом, время и деньги.

Необходимость использования коммутаторов

Перестройка сетевой инфраструктуры с целью интегрирования сегментных коммутаторов сети Ethernet в традиционно некоммутируемую сетевую среду может дать поразительные результаты не только с точки зрения повышения производительности сети, но и с точки зрения возможности использования устройств с низким соотношением цена/производительность, которые потребуют применения коммутации в отличие от сети FDDI, Fast Ethernet и других высокоскоростных сетевых технологий. Преимущества коммутации Ethernet налицо: она является относительно недорогой по сравнению с другими методами, дает ощутимое повышение производительности, поддерживает возможность восстановления полосы пропускания и режим полнодуплексной передачи данных. Коммутация может быть реализована за более короткий срок по сравнению с сети FDDI, Fast Ethernet и другими высокоскоростными сетевыми технологиями, позволяя сохранить при этом вложения в существующую сетевую

инфраструктуру. Как бы там ни было, перспектива возникновения сетевых заторов делает такое решение вполне приемлемым.

Как же работают коммутаторы? В широком смысле основная функция коммутаторов сети Ethernet заключается в разбиении больших перегруженных сетей на более управляемые подсети меньших масштабов. Для того чтобы избежать ситуации, когда устройство должно ожидать своей очереди на право передачи данных по перегруженному сегменту Ethernet 10Мбит/с, коммутаторы выделяют каждому из устройств (или группе устройств) "собственный" сегмент Ethernet 10Мбит/с, подключенный непосредственно к быстродействующему коммутатору, который и устанавливает межсегментные соединения. И хотя этот метод очень похож на использование мостов, существует несколько важных отличий, которые превращают коммутаторы в более динамичное и полезное аппаратное обеспечение.

Коммутаторы, если рассматривать их как обычные сетевые устройства, на первый взгляд не отличаются от маршрутизаторов, концентраторов и мостов ничем особенным. Однако существует три важных фактора, выгодно отличающих коммутаторы от своих коллег: общее быстродействие (коммутаторы намного быстрее), способ передачи данных или электронная логика (коммутаторы более интеллектуально подходят к этому вопросу) и возможность подключения большего числа устройств. В отличие от мостов и маршрутизаторов, которые обычно используют менее эффективные и более дорогие аппаратные и программные методы, коммутаторы пересылают кадры данных по различным сегментам более быстрым и эффективным способом. Таких результатов можно добиться только путем интенсивного использования интегральной логики, реализованной с помощью ASIC (Application-Specific Integrated Circuits - интегральных микросхем поддержки конкретных приложений).

Так же, как и мосты, коммутаторы разделяют большие сети на подсети и в значительной степени сокращают объем трафика между сегментами. В случае межсегментного трафика коммутаторы направляют кадры только через те сегменты, которые принадлежат хостам отправителя и получателя. Если в

инфраструктуре сети Ethernet коммутаторы отсутствуют, то как только одно устройство начнет передачу данных по сети, во избежание сбоев в работе другим устройствам будет откачано в доступе к среде передачи (в соответствии со спецификациями IEEE 802.3). В результате можно гарантировать целостность данных, но общая производительность сети снизится. Посредством распределения потока данных по локальным сегментам коммутаторы предоставляют подключенным устройствам дополнительные возможности для доступа к среде передачи (увеличивая скорость передачи данных и снижая время задержки). Передача данных локальным сегментам будет запрещена до тех пор, пока кадры не будут получены хостом другого сегмента. В этом случае коммутатор проверяет адрес получателя и пересылает необходимые кадры только через предписанный сегмент, не загружая тем самым все остальные подключенные к коммутатору сегменты. Теоретически эти сегменты могут продолжать обработку локального трафика. Итак, коммутаторы не только устанавливают пассивные связи между сегментами, но и пытаются снизить количество сегментов, занятых обработкой сетевого трафика.

Характеристики коммутаторов

Надеемся, что читатель уже убедился в той важной роли, которую могут играть коммутаторы сети Ethernet. Если же нет, попытайтесь перечитать все вышесказанное еще раз. Коммутаторы в состоянии спасти сеть, оказавшуюся на грани развала.

Если же принято решение реализовать идею коммутации то, возникает логичный вопрос: как выбрать коммутатор, удовлетворяющий всем заданным требованиям. Чтобы получить ответ, необходимо потратить некоторое время на изучение наиболее важных характеристик и принципов действия этих устройств. Собрав всю необходимую информацию, сделать правильный выбор уже не составит труда.

Статические и динамические коммутаторы

Если самый критичный участок сети уже известен и некоторые специалисты советуют приобрести статические коммутаторы, отнеситесь к подобным

рекомендациям с определенной долей недоверия. Независимо от того, являются ли статическими коммутаторами устройства, которые предполагается использовать для модернизации сети, обратите особое внимание на их функциональные возможности. Даже если устройство рекламируется как новейшее достижение информационных технологий, на практике от него может быть пользы не больше, чем от обычного концентратора. Стоит задача осуществления эффективного управления межсегментным трафиком с целью уменьшения числа критичных участков сети, а статические коммутаторы не смогут удовлетворить всем этим требованиям.

Совсем иначе дело обстоит с динамическими коммутаторами. Эти устройства не только уделяют особое внимание пересылке кадров по предписанному адресу, но и обрабатывают таблицу соответствий отдельных узлов конкретным портами, к которым они подключены. Эта информация обновляется каждый раз, как только очередная машина начинает передачу данных (или же через заранее заданные интервалы времени). Таблица постоянно обновляющихся комбинаций узел/порт предоставляет коммутатору возможность быстро направлять пакеты через соответствующие сегменты.

Динамические коммутаторы позволяют экономить время и силы в течение еще довольно продолжительного времени. Поскольку эти устройства обновляют свои таблицы соединений каждый раз, когда устройства начинают передачу, можно переупорядочить сеть, переключая рабочие станции на разные порты до тех пор, пока сеть не будет сконфигурирована оптимальным образом. (Учтите, что этим можно заниматься до посинения.) Таблицы будут обновляться автоматически, и сеть будет в полном порядке.

Сегментные и портовые коммутаторы

В настоящий момент ведутся горячие дебаты по поводу того, какие коммутаторы смогут решить проблему перегрузок в сети: сегментные или портовые. Все сводится к их стоимости. Если располагаете достаточными средствами, приобретите портовые коммутаторы. Если же нет - придется довольствоваться сегментными. Чем бы эти дебаты ни завершились, вы не

останетесь внакладе в любом случае.

Сегментные коммутаторы в состоянии управлять трафиком сегментов, подключенных к каждому порту, что в свою очередь предоставляет возможность соединять большее количество рабочих станций или сегментов, используя для этого меньшее количество коммутаторов/физических портов. Одной из самых важных особенностей сегментных коммутаторов является возможность обработки отдельной рабочей станции на каждом порту (которую можно рассматривать как сегмент, состоящий из одного узла). Специалист получает возможность заранее объединить в один сегмент машины, требующие лишь ограниченного доступа к сети, воспользовавшись для этого одним каналом с относительно низкой пропускной способностью 10 Мбит/с. В то же время современные устройства, например, сетевые серверы и серверы баз данных, оптические дисководы и т. д., могут подключаться по схеме "одно устройство/один порт", что позволяет этим широкополосным и критичным устройствам пользоваться правом индивидуального доступа к сети. Преимущества использования сегментных коммутаторов возрастает с тем обстоятельством, что их установка не требует дополнительных расходов на аппаратное обеспечение, проводку и т. д.

Портовые коммутаторы (иногда их называют коммутаторы-концентраторы) предназначены для ретрансляции данных, передаваемых отдельным устройством во все физические порты. Сетевые администраторы уже давно мечтают о возможности выделения каждой рабочей станции, серверу и всем остальным устройствам для доступа к сетевым ресурсам отдельного канала 10 Мбит/с. Однако использование портовых коммутаторов связано с дополнительными расходами на проводку (необходимо будет проложить кабель от каждого устройства к коммутатору), а также на закупку коммутаторов, требуемых для обеспечения необходимого количества физических портов. Кроме того, по мере роста сети неизбежно придется столкнуться с новыми, порой немалыми тратами, поскольку необходимость прокладки новых кабелей и приобретения новых коммутаторов будет возникать каждые несколько месяцев. Но какой бы путь вы

ни избрали, все равно будет создана сеть гораздо более совершенная по сравнению с той, в которой коммутаторы отсутствовали.

Коммутация без буферизации пакетов

Несмотря на то, что использование коммутаторов значительно повышает производительность сети, в некоторых случаях может возникнуть желание (или необходимость) выжать из системы нечто большее. Для этого можно реализовать метод коммутации без буферизации пакетов (cut-through switching).

Отказ от буферизации позволяет повысить производительность сети, поскольку пересылка пакетов будет осуществляться значительно быстрее по сравнению с традиционными конфигурациями. Выигрыш в производительности достигается благодаря тому, что пересылка данных машине получателя начинается еще до того, как пакет будет принят полностью - передача начинается сразу же после определения коммутатором адреса получателя. Несмотря на то, что этот метод значительно снижает сетевые задержки, отказ от буферизации позволяет засорять полосу пропускания большому количеству пакетов, содержащих ошибки. Для того чтобы этого избежать, следует настроить коммутатор таким образом, чтобы задержка между получением и отправлением пакета была максимальной. В идеальном случае сразу же после получения пакета коммутатор буферизирует 64 байта с целью исключения возможности появления ошибок в пакетах. После того как вероятность возникновения ошибок будет снижена, коммутатор сможет начать пересылку пакетов через соответствующий сегмент к хосту получателя. Это несколько увеличит время задержки, но скорость работы все равно будет выше, чем в случае использования обычных коммутаторов. К сожалению, если сеть чрезвычайно перегружена, применение этого метода будет менее эффективно по сравнению с применением других методов. Чем интенсивнее загружена сеть, тем быстрее сводятся на нет все преимущества коммутации без буферизации пакетов.

Коммутация с промежуточной буферизацией

Устройства, поддерживающие режим коммутации с промежуточной

буферизацией (store-and-forward switching), принципиально отличаются от коммутаторов, игнорирующих возможность буферизации. Устройства двух рассматриваемых типов можно сравнить с черепахой и зайцем, причем в роли черепахи будут выступать коммутаторы с промежуточной буферизацией.

В отличие от не использующих буферизацию коммутаторов, уделяющих основное внимание скорости передачи и отсылающих пакет при первой же возможности, буферизирующие коммутаторы полностью принимают пакет и лишь затем отсылают его по назначению. В результате коммутатор получает возможность проверить циклический избыточный код пакетов и обнаружить возникшие в процессе передачи ошибки, обеспечивая тем самым более надежную пересылку данных по сети. Пусть этот метод практически не повышает производительность сети, зато он позволяет исключить дополнительный поток данных, необходимый для устранения ошибок в пакетах, который в свою очередь требовал бы дополнительных сетевых ресурсов. Таким образом, использование этого метода в конечном счете все-таки позволяет увеличить скорость работы сети.

Другие аспекты коммутации

Существует множество различных аспектов коммутации, на которые следует обратить внимание приступая к модернизации сети. В предыдущих разделах мы все время ходили вокруг да около "актуальной" проблемы выбора коммутатора вместо того, чтобы тщательно рассмотреть работу сетей с целью создания более производительной и функционально законченной инфраструктуры. В следующих разделах будут кратко описаны высокоскоростные интерфейсы, методы администрирования сетей, высокоскоростные разновидности Ethernet и принципы построения виртуальных сетей. Применив все эти методы в совокупности, вы обнаружите, что производительность сети превзошла все ваши ожидания.

В случае развертывания (или модернизации) сети с помощью высокоскоростных коммутаторов особое внимание следует уделить вопросам усовершенствования и стандартизации максимального количества сетевых

соединений, исходя при этом из существующего аппаратного обеспечения и выделенных финансовых средств. Помимо хост-адаптеров в каждом из рассмотренных ранее примеров необходимо было обеспечить соответствующую проводку типа CAT5. В процессе маршрутизации задействовано три типа узлов: серверы, рабочие станции и присоединенные к ним устройства, а также межкоммутационные соединения.

Поскольку сетевой адаптер сервера наиболее подвержен перегрузкам, необходимо обеспечить поддержку сервером одного из высокоскоростных интерфейсов. Поскольку быстродействие сети определяется быстродействием наиболее инертной ее части, следует обратить внимание на тот факт, что применение хост-адаптеров (которые, кстати, легче всего модернизируются) не снизит производительность. Одновременно это позволит повысить скорость обмена данными с сервером.

В качестве второго фактора, влияющего на производительность сети, следует рассматривать характеристики рабочих станций и других подключенных к сети устройств. В частности, особое внимание следует уделить типу и производительности сетевых адаптеров, которые широко используются в рабочих станциях. Применение высокоскоростных адаптеров-интерфейсов имеет большое значение, поскольку обеспечивает быструю передачу данных и более оперативную связь между коммутаторами и серверами, а также позволяет за более короткое время освободить сеть для других устройств. К тому же производительность сети, несмотря на преимущества коммутации, будет страдать из-за значительной разницы в быстродействии интерфейсов различных сетевых устройств. Это вызвано тем, что быстрые порты не могут начать работу прежде, чем закончат прием от медленного порта, который в свою очередь в состоянии полностью использовать полосу пропускания, поддерживаемую быстрым портом. Можно сказать, что быстрый порт находится как бы во власти медленного.

Поскольку вопрос поддержки серверами и рабочими станциями высокоскоростных интерфейсов имеет большое значение, важно удостовериться в том, что скорость передачи данных между коммутаторами соответствует

предъявляемым ей требованиям. В конечном счете модернизация сети окажется совершенно бесполезной, если в самих коммутаторах будут возникать еще большие заторы, чем те, которых вы пытались с их помощью избежать.

Повышение скорости межкоммутационного соединений -отнюдь не самая большая из всех проблем, с которыми придется столкнуться при внедрении коммутаторов в сеть, поскольку в большинстве случаев будет достаточно использования лишь одного коммутатора (не менее распространена ситуация, когда коммутаторы вынуждены поддерживать изолированные сегменты). Однако если возникнет необходимость использования межкоммутационных соединений, между ними придется создать высокоскоростную мини-магистраль. С целью обеспечения приемлемой полосы пропускания и низкого времени задержки доступа к сети используются наиболее быстрые интерфейсы и качественная проводка.

Можно выделить два наиболее эффективных направления в развитии сетей Ethernet, заслуживающих особого внимания при рассмотрении вопроса коммутации. Использование этих технологий позволяет значительно повысить общую производительность сетей и не влечет за собой больших затрат на аппаратное обеспечение.

Разработка коммутируемых сетей Ethernet, предполагающих использование портовых и сегментных коммутаторов в сочетании с полнодуплексным режимом передачи в сети Ethernet (20 Мбит/с) обеспечивает повышение общей производительности сетей и в значительной степени снижает сетевые задержки. Это позволяет создать для пользователей более чувствительную сеть. Полнодуплексный режим работы сети Ethernet реализуется путем отключения процедур определения конфликтов, которые являются частью традиционной (полудуплексной) схемы Ethernet CSMA/CD. Использование этого режима в уже существующей кабельной инфраструктуре позволит сохранить значительную часть средств, инвестируемых в развитие сети. Безусловно, этот факт можно считать преимуществом в любом случае. Однако если использование полнодуплексного режима не требует замены существующей проводки, для персональных

компьютеров, сетевых и других серверов, а также для остальных устройств придется использовать новые высокоскоростные сетевые адаптеры.

Другой прогрессивной технологией, в значительной степени, повышающей скорость передачи данных по сети, является быстрый Ethernet (Fast Ethernet). Эта новейшая система позволяет передавать данные по сети со скоростью 100 Мбит/с и выше, что значительно превышает скорость передачи в традиционных сетях Ethernet (10 Мбит/с) или в сетях Token Ring (4 или 16 Мбит/с). Быстрый Ethernet допускает использование кабелей третьей и пятой категорий, хотя в данном случае предпочтительнее выглядит категория CAT5 (как обладающая низким значением соотношения сигнал/шум и соответственно более надежная).

Как уже отмечалось, сильнее всего подвержены сетевым перегрузкам именно сетевые серверы. Использование коммутации будет первым шагом на пути к решению такого рода проблем. Однако в случае объединения методов коммутации и преимуществ быстрого Ethernet можно было бы получить такую производительность, которую не смогла бы обеспечить ни одна из вышеупомянутых технологий, взятая в отдельности.

Если же перед вами встала необходимость модернизации проводки, реализация быстрого Ethernet будет недорогим и легче всего осуществимым способом, обеспечивающим скорость передачи данных порядка 100 Мбит/с. Применение ATM, FDDI и ADSL также принесет неплохие результаты. Однако в этом случае придется вложить значительные средства и потратить немало времени на подготовку персонала и развертывание самой сети.

При выборе коммутатора в первую очередь необходимо удостовериться в том, что производитель поддерживает (или собирается поддерживать) SNMP-совместимые средства управления (см. гл. 1), которые позволят вам эффективно отслеживать и разрешать все проблемы, связанные с использованием приобретаемых устройств. И хотя предоставляемые в распоряжение сетевого администратора ресурсы будут в некоторой степени отличаться (в зависимости от изготовителя устройства), убедитесь в том, что в документации к приобретаемому коммутатору приведена информация о производительности, погрешности и других

характеристиках. Это поможет в дальнейшем определить причину возможных неполадок и устранить их.

Топология клиент/сервер.

Клиент-сервер (англ. *Client-server*) — вычислительная или сетевая архитектура, в которой задания или сетевая нагрузка распределены между поставщиками услуг, называемыми серверами, и заказчиками услуг, называемыми клиентами. Нередко клиенты и серверы взаимодействуют через компьютерную сеть и могут быть как различными физическими устройствами, так и программным обеспечением.

Преимущества:

- Отсутствие дублирования кода программы-сервера программами-клиентами.
- Так как все вычисления выполняются на сервере, то требования к компьютерам, на которых установлен клиент, снижаются.
- Все данные хранятся на сервере, который, как правило, защищён гораздо лучше большинства клиентов. На сервере проще обеспечить контроль полномочий, чтобы разрешать доступ к данным только клиентам с соответствующими правами доступа.

Недостатки:

- Неработоспособность сервера может сделать неработоспособной всю вычислительную сеть. Неработоспособным сервером следует считать сервер, производительности которого не хватает на обслуживание всех клиентов, а также сервер, находящийся на ремонте, профилактике и т. п.
- Поддержка работы данной системы требует отдельного специалиста — системного администратора.
- Высокая стоимость оборудования.

Многоуровневая архитектура клиент-сервер

Многоуровневая архитектура клиент-сервер — разновидность архитектуры

клиент-сервер, в которой функция обработки данных вынесена на один или несколько отдельных серверов. Это позволяет разделить функции хранения, обработки и представления данных для более эффективного использования возможностей серверов и клиентов.

Частный случай многоуровневой архитектуры:

Трёхуровневая архитектура, или трёхзвённая архитектура (англ. *three-tier* или англ. *Multitier architecture*) — архитектурная модель программного комплекса, предполагающая наличие в нём трёх компонентов: *клиентского приложения* (обычно называемого «тонким клиентом» или терминалом), *сервера приложений*, к которому подключено клиентское приложение, и *сервера базы данных*, с которым работает сервер приложений.

Сеть с выделенным сервером

Сеть с выделенным сервером (англ. *Client/Server network*) — это локальная вычислительная сеть (LAN), в которой сетевые устройства централизованы и управляются одним или несколькими серверами. Индивидуальные рабочие станции или клиенты (такие, как ПК) должны обращаться к ресурсам сети через сервер(а).

2.4. Коммуникационные системы в создании виртуальных локальных сетей

Телекоммуникационная среда локальной сети

В случае если тщательный анализ функциональной структуры сети, с применением эффективных коммутаторов и широкой инсталляцией поддержки высокоскоростных интерфейсов не принесли ожидаемых результатов в виде повышения уровня производительности, необходимо следующее. Это еще один вариант решения этой проблемы, который, возможно, потребует затратить гораздо больше времени и сил. Однако если сеть очень громоздка и напичкана большим количеством коммутаторов, нельзя не обойтись без коммуникационной технологии создания виртуальных сетей.

Вполне возможно, что уже имеется какое-то представление о принципах

организации виртуальных сетей. Их создание сводится к выделению из одной физической сети определенного числа логических сетей или к группированию сегментов, подключенных к одному коммутирующему устройству. Это осуществляется путем настройки коммутатора, который представит определенным рабочим станциям или сегментам доступ лишь к заданным сегментам, запрещая тем самым доступ ко всем остальным, соединенным с коммутатором сегментам (рис. 2.20).

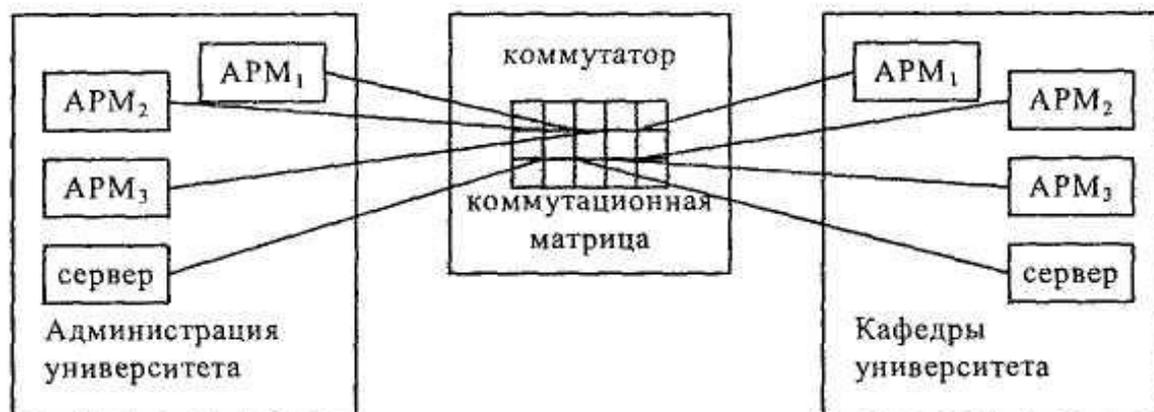


Рис. 2.20 Технология соединения коммутатора с сегментами сети.

Организация виртуальных сетей может использоваться в качестве средства администрирования и безопасности, позволяющего администратору группировать сегменты в логические сети в зависимости от расположения в здании (например, по отделам организации) или просто с целью разгрузки переполненных участков сети. Более того, с помощью виртуальных сетей можно предоставить доступ к ограниченному количеству сегментов лишь пакетам заранее определенных хостов.

Хостинг (англ. *hosting*) — услуга по предоставлению вычислительных мощностей для размещения информации на сервере, постоянно находящемся в сети (обычно Интернет). Хостингом также называется услуга по размещению оборудования клиента на территории провайдера с обеспечением подключения его к каналам связи с высокой пропускной способностью (колокация, от англ. *collocation*). Обычно хостинг входит в пакет по обслуживанию сайта и подразумевает как минимум услугу размещения файлов сайта на сервере, на котором запущено ПО, необходимое для обработки запросов к этим файлам (веб-сервер). Как правило, в обслуживание уже входит предоставление места для почтовой корреспонденции, баз данных, DNS, файлового хранилища на специально выделенном файл-сервере и т. п., а также поддержка функционирования соответствующих сервисов. Хостинг базы данных, размещение файлов, хостинг электронной почты, услуги DNS могут предоставляться отдельно как самостоятельные услуги, либо входить в

комплексную услугу.

Хост (от англ. *host* — «хозяин, принимающий гостей») или **узел** — любое устройство, предоставляющее сервисы формата «клиент-сервер» в режиме сервера по каким-либо интерфейсам и уникально определённое на этих интерфейсах. В более частном случае под хостом могут понимать любой компьютер, сервер, подключённый к локальной или глобальной сети. Иногда при упоминании конкретного устройства в сети, также используют термин "узел" (очевидно, по аналогии с прототипом компьютерной сети, ведь реальная сеть, например рыболовная, состоит из нитей, соединённых между собой множеством узлов).

Слово «хост» само по себе является практически жаргонным термином, и не несёт никакой информации об устройстве или его функционировании. Употребление слова «хост» имеет смысл только вместе с пояснением, хостом *какого* сервиса предполагается называемое устройство. Тем не менее, зачастую название сервиса опускают, предполагая, что оно очевидно из **контекста**.

Таким образом, поток данных от потенциально опасных машин будет прекращен задолго до того, как эти машины начнут создавать угрозу для общих данных или производительности сети.

Коммуникационная технология виртуальных сетей (Virtual LAN) является одним из наиболее перспективных аспектов коммутируемых сетей. Виртуальные ЛВС являются необходимым элементом корпоративных коммутируемых сетей, обеспечивая переход от сетей с разделяемой средой к полностью коммутируемым системам.

В современных сетях четко прослеживается тенденция перехода от систем с разделяемой средой на базе концентраторов к использованию коммутаторов для соединения рабочих станций и сетевых ресурсов. Однако коммутаторы работают на канальном уровне модели OSI и являются устройствами рассылки кадров, которые неспособны обеспечить достаточно эффективное масштабирование крупных сетей. В традиционных сетях на основе концентраторов и маршрутизаторов пользователи группируются в широковещательные домены (сегменты), для соединения которых служат маршрутизаторы. Такое решение позволяет всем пользователям в группе разделять полосу своего концентратора или кольца и снижает уровень насыщения полосы и число коллизий за счет уменьшения числа пользователей в каждом сегменте. Коммутируемые сети не имеют

широковещательных доменов, поэтому производительность сети снижается за счет широковещательного трафика, особенно при использовании таких протоколов, как IPX. Виртуальные ЛВС позволяют организовать в коммутируемой сети широковещательные домены, обеспечивая тем самым возможность эффективного масштабирования.

Виртуальные ЛВС имеют и другие преимущества - они позволяют более эффективно использовать IP-адреса, существенно упрощают перенос станций или ресурсов в пределах сети, обеспечивают более эффективную организацию пользователей по группам.

По мере развития коммутационных технологий были предложены многочисленные варианты организации коммутируемых сетей. Разные варианты построения VLAN имеют свои преимущества и недостатки. Ниже рассмотрены некоторые аспекты использования виртуальных сетей и требования к их организации и поддержке.

Коммутаторы ЛВС обеспечивают высокую производительность за счет процессов, схожих с используемыми в традиционных мостах. Коммутаторы используют адреса канального уровня (MAC-адреса) для определения порта, в который требуется передать пакет. Работа с адресами канального уровня много проще и быстрее по сравнению с маршрутизацией, использующей протоколы сетевого уровня. В отличие от маршрутизации рассылка кадров на канальном уровне (коммутация) не требует изменения содержимого кадров, тогда как маршрутизаторы вынуждены добавлять в пакеты адреса и счетчик интервалов. Кроме того, маршрутизаторы должны поддерживать еще целый ряд функций - выбор маршрута, преобразование адресов и т.п. - при перемещении данных по сети. Не следует забывать и о том, что в большинстве сетей используется несколько протоколов - следовательно маршрутизатор должен обеспечивать работу со всеми протоколами и передавать данные для разных протоколов через сеть.

В использовании устройств канального уровня для построения виртуальных сетей нет ничего нового. Первые ЛВС создавались на основе простых мостов. Основное отличие коммутаторов от традиционных мостов

заключается в производительности обработки пакетов и поддержке интенсивных потоков трафика.

Однако всем коммутируемым сетям присуще одно ограничение. Поскольку коммутатор не имеет дел с протоколами сетевого уровня, он не может знать куда направлять широковещательные пакеты. Хотя трафик с конкретными адресами (соединения «точка-точка») изолирован парой портов, широковещательные пакеты передаются во всю сеть (каждый порт). То же самое происходит в случае с пакетами, предназначенными станции с неизвестным MAC-адресом, - такие пакеты просто передаются всем. Однако, широковещательные пакеты и пакеты с неизвестными адресами могут привести к насыщению полосы и росту числа коллизий, особенно в крупных сетях.

В некоторых сетях средних размеров с невысоким уровнем широковещательного трафика кадры, передаваемые всем (т. н. лавинная маршрутизация), почти не влияют на картину трафика - число широковещательных пакетов невелико, а неизвестные адреса достаточно быстро выясняются коммутатором. Однако в больших сетях (или небольших, но с высоким уровнем широковещательного трафика) ситуация может оказаться совершенно иной и рассылка широковещательных пакетов во все порты может свести на нет все преимущества коммутации. Для того, чтобы этого не происходило важно ограничить область распространения широковещательного трафика - организовать небольшие широковещательные домены или виртуальные ЛВС. В сетях на базе маршрутизаторов каждый порт маршрутизатора является широковещательным доменом. Для коммутаторов требуется возможность поддержки широковещательного трафика без снижения производительности. Для того, чтобы добиться этого производители коммутаторов предлагают создавать виртуальные ЛВС (VLAN), являющиеся просто широковещательными доменами. Виртуальные сети обеспечивают сегментацию за счет создания логических, динамических широковещательных доменов. Более того, виртуальные ЛВС существенно расширяют возможности масштабирования сетей.

2.4.2. Типы телекоммуникационных сред

Формирование коммуникационной среды для виртуальной сети должно начинаться с выбора коммутатора. Одновременно с этим администратор должен решить, кого из пользователей следует подключить напрямую к коммутатору. До появления коммутаторов пользователи вынужденно группировались по своему местоположению в ширококвещательные домены. С появлением коммутаторов и виртуальных сетей стало возможным объединение пользователей в логические группы на основе функциональных обязанностей, протоколов, используемых приложений и т.п.

Здесь нет ничего нового, такие же методы используются в традиционных сетях на базе концентраторов и маршрутизаторов. Однако в традиционных сетях трафик является ширококвещательным внутри образующего сегмент концентратора и маршрутизируется между концентраторами. При использовании виртуальных сетей кадры являются ширококвещательными внутри VLAN и маршрутизируются между ними. Таким образом виртуальные сети представляют собой ни что иное, как более гибкий вариант традиционных ЛВС с несколько большими возможностями.

Мощь и гибкость являются атрибутами виртуальных сетей в хороших реализациях. Ширококвещательные домены больше не ограничены одним портом маршрутизатора - сейчас ширококвещательный домен может быть объединять устройства, подключенные к одному или нескольким портам коммутатора или даже к портам разных коммутаторов. VLAN организуются на базе логических групп пользователей - расположение пользовательских станций больше не имеет значения. Это важный момент. В сетях на основе маршрутизаторов и концентраторов группы пользователей жестко определялись местоположением последних. Для обмена между станциями в результате приходилось передавать большие потоки данных через маршрутизаторы. При организации логических

групп потоки данных через маршрутизаторы можно уменьшить во много раз.

Коммуникационные среды виртуальных сетей при использовании достаточно эффективных решений способны сделать картину сетевого трафика значительно более эффективной. Если пользователи сгруппированы в широковещательные домены так, что большая часть трафика остается внутри группы, нагрузка на магистрали и маршрутизаторы существенно снижается. Широковещательный домен может содержать компьютеры, находящиеся в одном здании, городе или даже на значительном удалении друг от друга при поддержке виртуальных ЛВС с использованием WAN-каналов. Поскольку при обмене данными внутри группы маршрутизаторы не используются, обмен между станциями происходит гораздо быстрее.

Сегодня существует достаточно много вариантов коммуникационных сред для VLAN. Простые варианты этих сред для VLAN представляют собой просто набор портов коммутатора, более сложные реализации позволяют создавать группы на основе других критериев. В общем случае возможности организации VLAN тесно связаны с возможностями коммутаторов.

Ниже рассматриваются шесть основных типов коммуникационных сред для VLAN.

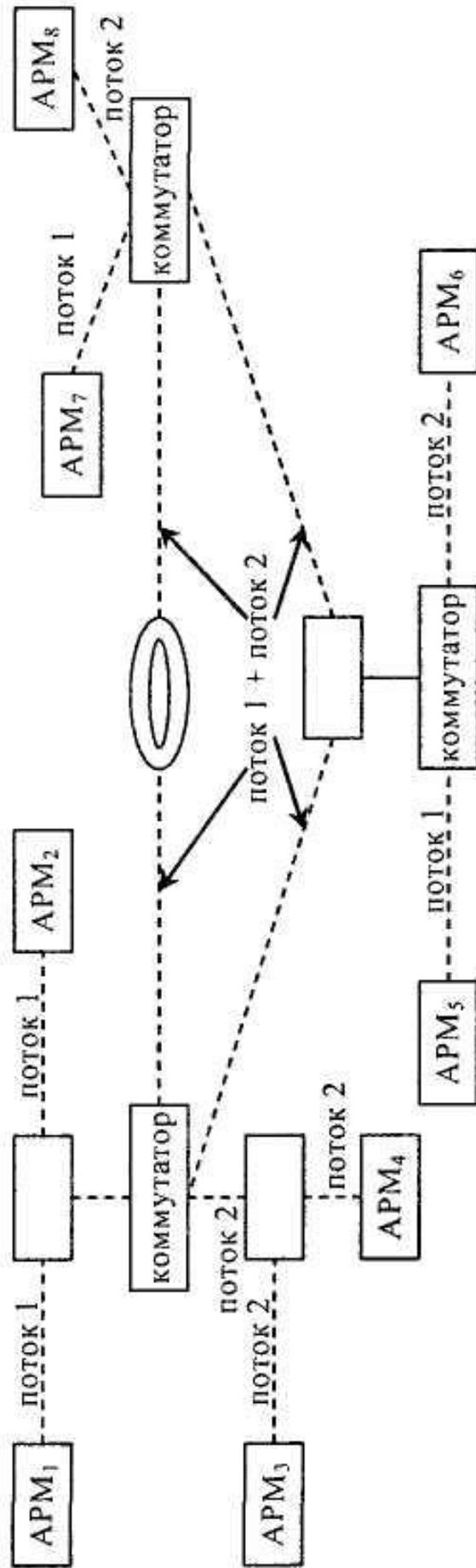


Рис. 2.21. Коммуникационная среда для сети с коммутаторами на основе портов.

Коммуникационная среда для сети с коммутатором на основе портов

Это простейший вариант организации виртуальной ЛВС. ЛВС (VLAN) на базе портов обеспечивают высочайший уровень управляемости и безопасности. Устройства связываются в виртуальные сети на основе портов коммутатора, к которым эти устройства физически подключены. VLAN на базе портов являются статическими и для внесения изменений требуется физическое переключение устройств (рис. 2.21).

Однако построенные на базе портов виртуальные сети имеют некоторые ограничения. Они очень просты в установке, но позволяют поддерживать для каждого порта только одну виртуальную ЛВС. Следовательно, такое решение малоприменяемо при использовании концентраторов или в сетях мощными серверами, к которым обращается много пользователей (сервер не удастся включить в разные VLAN). Кроме того, виртуальные сети на основе портов не позволяют вносить в сеть изменения достаточно простым путем, поскольку при каждом изменении требуется физическое переключение устройств.

Коммуникационная среда для сети на основе MAC-адресов

Хотя этот тип виртуальных сетей относится к числу наиболее простых, VLAN на базе MAC-адресов настраивать сложнее, нежели сети на основе физических портов. Виртуальная сеть на базе MAC-адресов группирует устройства в широковещательный домен (VLAN). Сети на базе MAC-адресов являются одним из наиболее безопасных и управляемых типов VLAN. Для получения доступа в виртуальную сеть, устройство должно иметь MAC-адрес, известный программе VLAN (рис. 2.22).

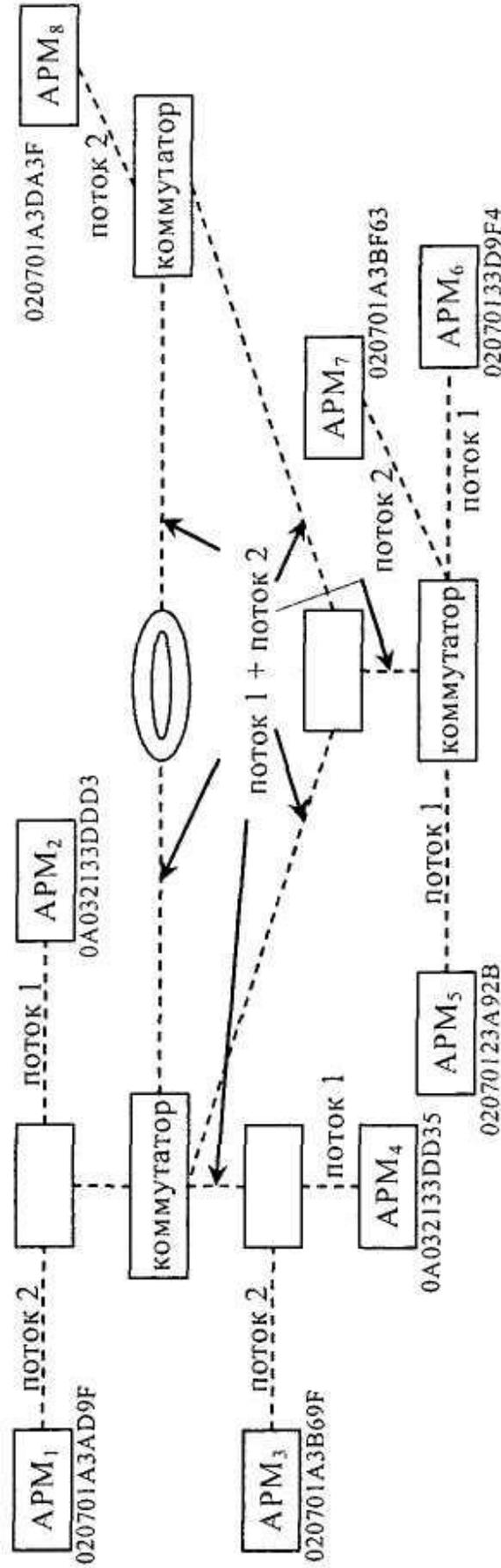


Рис 2 22 Коммуникационная среда для сети с коммутаторами на основе MAC-адресов

Настройка виртуальной сети на основе MAC-адресов может отнять много времени - представьте себе, что вам потребуется связать с VLAN адреса 1000 устройств. Кроме того, MAC-адреса «наглухо защиты» в оборудовании и может потребоваться много времени на выяснение адресов устройств в большой, территориально распределенной сети. Однако программа управления сетью позволяет собрать адреса в масштабе всей сети автоматически, избавляя администратора от рутинной работы. С помощью программы можно настроить виртуальные сети, используя вместо MAC-адресов связанные с ними имена станций.

Коммуникационная среда для сети на основе протоколов сетевого уровня

Виртуальные ЛВС сетевого уровня позволяют администратору связать трафик для того или иного протокола в соответствующей виртуальной сети. Точно таким же способом создаются широковежательные домены в сетях на основе маршрутизаторов. Протокол может быть задан в форме IP-подсети или сетевого номера IPX. Можно, к примеру, объединить в виртуальную ЛВС всех пользователей подсети, которая была организована до использования коммутаторов.

Спектр возможностей коммутатора, на базе которого строится VLAN, часто определяет гибкость виртуальных сетей данного типа. Многие виртуальные ЛВС сетевого уровня поддерживают системы на базе нескольких коммутаторов, тогда как другие могут работать только с одним устройством. Помните, что этот тип виртуальных ЛВС почти не отличается от сетей на базе маршрутизаторов и некоторые коммутаторы неспособны обеспечить требуемую в данном случае производительность. Коммутаторы хорошо справляются с задачами этого типа.

Коммуникационная среда для сети на основе заданных протоколов

Этот тип виртуальных сетей строится на базе заданного в каждом кадре типа протокола. Такой подход позволяет администратору задать критерии, по которым Auto Tracker будет создавать VLAN. Администратор может самостоятельно выбрать поля в заголовках кадров, по которым будет определяться принадлежность к виртуальной сети, и загрузить подготовленные правила во все коммутаторы сети. Вы можете поместить в одну виртуальную сеть всех пользователей, работающих с протоколом Net Bios или IP. Для работы с данным типом виртуальных сетей администратор должен досконально разбираться в заголовках широковещательных кадров (рис. 2.23).

После того, как правила (параметры протокола) загружены в коммутаторы Omni Switch или Pizza Switch, устройства сразу же позволяют начать работу с виртуальными сетями на основе заданных администратором параметров протокола.

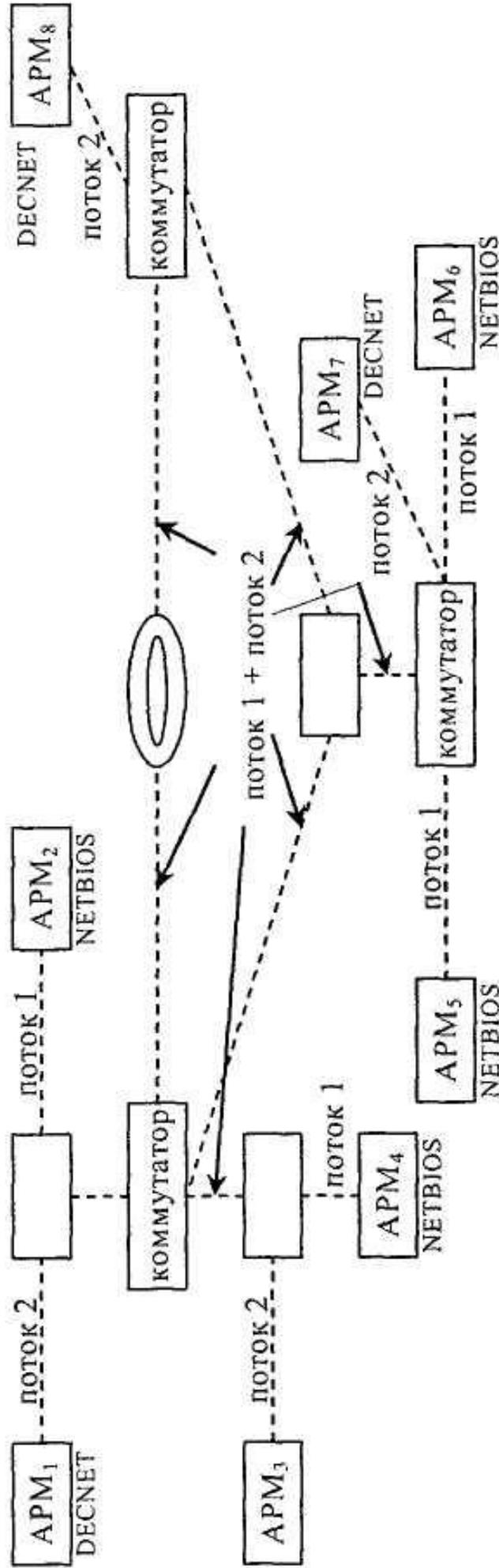


Рис. 2.23. Коммуникационная среда сети с коммутаторами на основе заданных протоколов.

Коммуникационная среда для сети на основе заданных специальных правил

Это наиболее мощная реализация VLAN, позволяющая администратору использовать любые комбинации критериев для создания виртуальных ЛВС. Для включения устройств в виртуальные ЛВС можно использовать все перечисленные выше способы при условии их поддержки установленными в сети коммутаторами. После того, как правила загружены во все коммутаторы, они обеспечивают организацию VLAN на основе заданных администратором критериев. Поскольку в таких сетях кадры постоянно просматриваются на предмет соответствия заданным критериям, принадлежность пользователей к виртуальным сетям может меняться в зависимости от текущей деятельности пользователей (рис. 2.24).

Виртуальные ЛВС на основе правил используют широкий набор критериев принадлежности к сети, включая все перечисленные выше варианты: MAC-адреса, адреса сетевого уровня, тип протокола и т. д. Возможно также использовать любые комбинации критериев для создания правил, наиболее точно соответствующих вашим задачам.

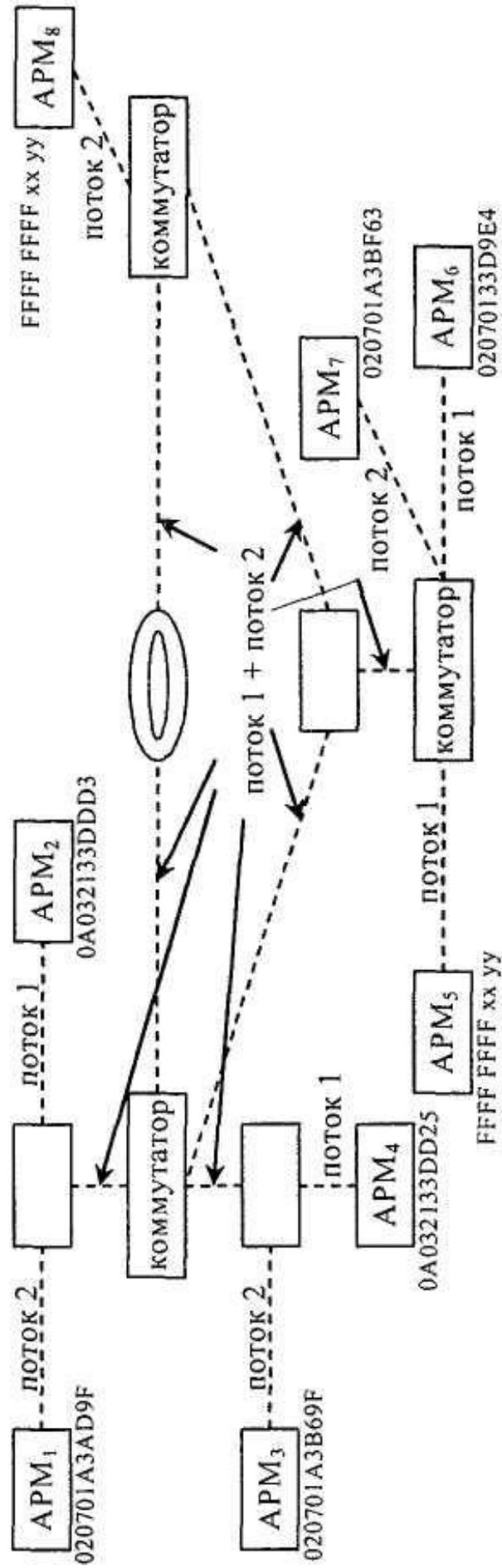


Рис. 2.24 Коммуникационная среда для сети с коммутаторами на основе заданных специальных правил

Коммуникационная среда для сети на основе формирования многоадресного (multicast) взаимодействия

Многоадресный трафик отличается от широковещательного, который передается во всю сеть, и одноадресного, обеспечивающего связь «точка-точка». Многоадресный трафик представляет собой обмен «точка-многоточка» (один со многими) или многоточечный (многие со многими) и в последнее время становится все более популярным для различных сетевых приложений. Многоадресный режим может использоваться для видеоконференций, биржевых систем, новостей и т.п. систем, где одна и та же информация передается многочисленным пользователям (рис. 2.25).

Виртуальные ЛВС с многоадресным трафиком создаются динамически путем прослушивания (ДПО - IGMP, Internet Group Management Protocol). Когда пользователь открывает приложение, использующее многоадресный режим, он динамически включается в виртуальную сеть, связанную с данным приложением. По окончании работы с программой пользователь удаляется из соответствующей виртуальной сети.

Многоадресный трафик в общем случае является стабильным потоком с достаточно широкой полосой. Следовательно, такой трафик лучше всего зафиксировать в одной виртуальной сети для предотвращения лавинной маршрутизации.

Задания, выполнение которых оценивает степень полученных знаний

2.1. Сформируйте схему функциональной структуры локальных сетей и дайте характеристику ее базовых компонент: серверов, автоматизированных рабочих мест (АРМ) - компьютеров пользователей.

2.2. Сформируйте схемы одноранговой и многогранговой организации локальных сетей и дайте характеристику преимуществ и недостатков для различных условий их применения.

2.3. Сформируйте схемы разных типов топологии: шинная, кольцевая, комбинированная, звездообразная и дайте характеристику преимуществ и недостатков для различных условий их

применения.

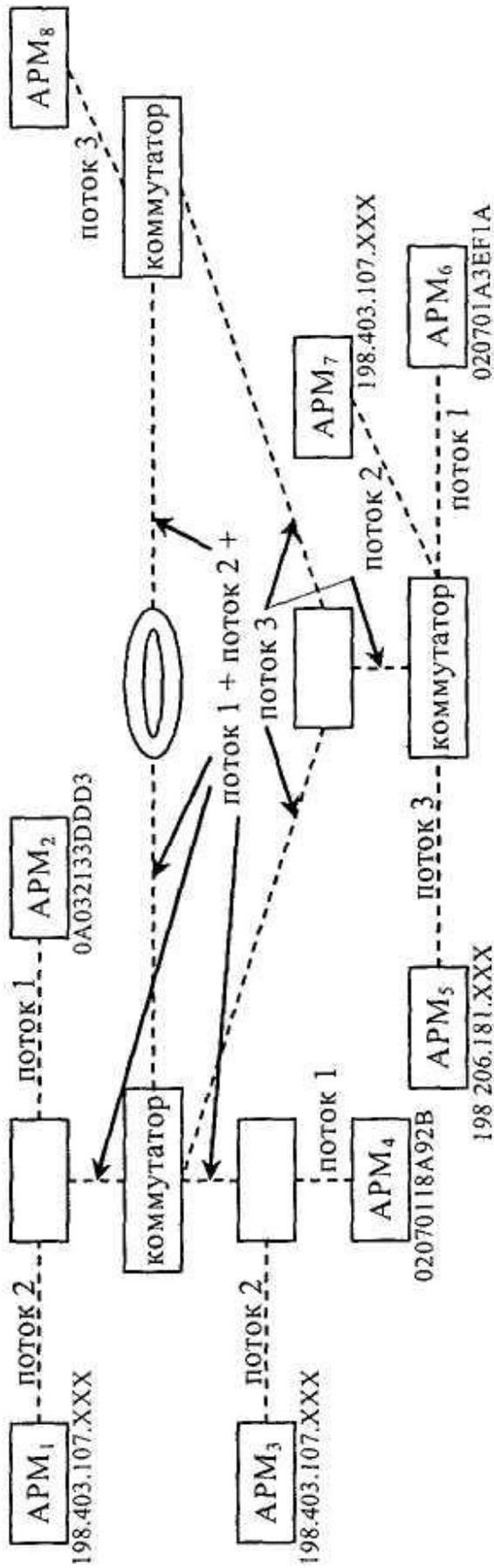


Рис. 2.25. Коммуникационная среда для сети с коммутаторами на основе многоадресного взаимодействия.

2.4. Сформируйте схемы разных типов топологии: коммутируемая, последовательных цепочек, иерархическая (кольца, звезды, комбинации), беспроводная (статическая и эпизодическая структуры) и дайте характеристику особенностей их применения.

2.5. Сформируйте схемы базовых коммутационных компонент: мостов и маршрутизаторов и дайте характеристику особенностей их применения.

2.6. Сформируйте схемы разных типов концентраторов: пассивные, активные, интеллектуальные и дайте характеристику особенностей их применения.

2.7. Дайте характеристику особенностей их применения коммутационных топологий: мостов, маршрутизаторов и специальных типов коммутаторов (динамических, сегментных, портовых с буферизацией и без буферизации), учитывающих мониторинг перегрузок сети.

2.8. Сформируйте схемы коммутационных сред на основе портов, MAC-адресов, протоколов сетевого уровня, заданных протоколов (или специальных правил) и многоадресного взаимодействия, дайте характеристику особенностей процессов коммутации.

Литература

1. ФлингД. Локальные сети ЭВМ. Архитектура, принципы построения. // М. «Финансы статистика» - 1986 - 360 с.
2. Соловьева Л.Ф. Сетевые технологии. // СПб. «БХВ-Петербург» - 2004 - 399 с.
3. Столинг СВ. Современные компьютерные сети. // СПб. «Питер» - 2003 - 784 с.
4. Тоненбаум Э. Компьютерные сети. // СПб. «Питер» - 2005 - 992 с.
5. Одом У. Компьютерные сети. // М. «Вильяме» - 2005 - 420 с.
6. Шиллер И. Мобильные коммуникации. // М. «Вильяме» - 2002 - 275 с.